
First Published: 2019-07-03
Last Modified: 2019-12-24

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883
# CONTENTS

## CHAPTER 1

### What's New for Cisco SD-WAN 1

- What's New for Cisco SD-WAN Release 19.2.x 1

## CHAPTER 2

### Policy Basics 3

- Policy Overview 3
- Policies in Cisco vManage 5

## CHAPTER 3

### Cisco SD-WAN Policy Framework Basics 11

- Cisco vSmart Policy Architecture Components 11
- Cisco vSmart Policy Operation 12
  - Control Policy Operation 13
  - Data Policy Operation 14
- VPN Membership Policy Operation 15
- Configure and Execute Cisco vSmart Policies 16
- Cisco vSmart Policy Components 17
- TLOC Attributes Used in Policies 19
- vRoute Attributes Used in Policies 20
- Cisco vSmart Policy Processing and Application 21

## CHAPTER 4

### Control Policies 23

- Centralized Control Policy 25
  - Configure the Network Topology 26
    - Hub and Spoke 26
    - Mesh 26
    - Custom Control (Route and TLOC) 27
  - Import Existing Topology 31
Create a VPN Membership Policy 31

Route Types 32

Default Behavior Without Centralized Control Policy 32

Behavior Changes with Centralized Control Policy 33

Examples of Modifying Traffic Flow with Centralized Control Policy 34

Create an Arbitrary Topology 34

Set Up Traffic Engineering 35

Configuration Components 37

Configure Centralized Policy Using Cisco vManage 38

Configure Centralized Policy Using CLI 44

Structural Components for Centralized Control Policy 45

Apply Centralized Control Policy 53

Centralized Control Policy Configuration Examples 54

Localized Control Policy 58

Configure Localized Control Policy Using Cisco vManage 59

Configure Localized Control Policy Using CLI 65

Structural Components for Localized Control Policy 66

Apply Route Policy for BGP 73

Apply Route Policy for OSPF 74

Device Access Policy 75

Device Access Policy Overview 76

Configure Device Access Policy Using vManage 76

Configure Device Access Policy Using CLIs 77

Verifying Device Access Policy Configuration 78

CHAPTER 5  Data Policies 81

Centralized Data Policy 82

Configure Centralized Data Policy Based on Prefixes and IP Headers 84

Start the Policy Configuration Wizard 84

Step 1: Create Policy Lists 85

Step 2: Configure Traffic Rules 88

Step 3: Apply Policies to Sites and VPNs 92

Step 4: Activate a Centralized Data Policy 93
# Configure Centralized Data Policy Using CLI

93

## Structural Components of Policy Configuration for Centralized Data Policy

94

- Lists 95
- VPN Lists 98
- Policer Parameters 98
- Sequences 98
- Match Parameters 99
- Action Parameters 100
- Default Action 104

## Apply Centralized Data Policy

104

## Deep Packet Inspection

105

- Configure Deep Packet Inspection Using vManage 105
- Configure Deep Packet Inspection Using CLI 107

## Structural Components of Policy Configuration for Deep Packet Inspection

109

- Action Parameters for Configuring Deep Packet Inspection 110
- Apply Centralized Data Policy for Deep Packet Inspection 113
- Configure VPN Membership Policy 114

## Centralized Data Policy Configuration Examples

116

## Localized Data Policy

119

## Localized Data Policy for IPv4

120

- Configure Localized Data Policy for IPv4 Using Cisco vManager 121
- Configure Localized Data Policy for IPv4 Using the CLI for Cisco vEdge Devices 135

## Localized Data Policy for IPv6

137

- Configure Localized Data Policy for IPv6 Using Cisco vManager 138
- Structural Components of Configuration for Access Lists 143
- Configure Localized Data Policy for IPv6 Using the CLI 149

## Localized Data Policy Configuration Examples

150

---

## Policy Basics CLI Reference

151

---

## Forward Error Correction

157

- Configure Forward Error Correction for a Policy 157
- Monitor Forward Error Correction Tunnel Information 158
- Monitor Forward Error Application Family Information 159

---

CHAPTER 8  
Packet Duplication for Noisy Channels  161
Configure and Monitor Packet Duplication  161
Configure Packet Duplication  161
Monitor Packet Duplication Per Application  162

CHAPTER 9  
Application-Aware Routing  163
Components of Application-Aware Routing  164
Classification of Tunnels into SLA Classes  165
Configure Application-Aware Routing  167
Configure ApplicationAware Routing Using CLIs  175
Structural Components of Policy Configuration for Application-Aware Routing  177
Apply Application-Aware Routing Policy  184
Configure the Monitoring of Data Plane Tunnel Performance  186
Application-Aware Routing Policy Configuration Example  187

CHAPTER 10  
Service Chaining  191
Service Chaining Configuration Examples  193

CHAPTER 11  
Traffic Flow Monitoring with Cflowd  201
Configure Cflowd Traffic Flow Monitoring  204
Configure Cflowd Traffic Flow Monitoring Using CLI  210
Structural Components of Policy Configuration for Cflowd  212
Apply and Enable Cflowd Policy  215
Cflowd Traffic Flow Monitoring Configuration Example  216

CHAPTER 12  
Cisco vEdge Device as a NAT Device  219
Cisco vEdge Device as a NAT Device on the Transport Side  219
Transport-Side NAT Operation  220
Cisco vEdge Device as a Service-Side NAT Device  222
Configure Local Internet Exit  223
Configure Service-Side NAT  227
Configure Split DNS  234
What's New for Cisco SD-WAN

This chapter describes what's new in Cisco SD-WAN for each release.

- What's New for Cisco SD-WAN Release 19.2.x, on page 1

What's New for Cisco SD-WAN Release 19.2.x

This section applies to Cisco vEdge devices.

Cisco is constantly enhancing the SD-WAN solution with every release and we try and keep the content in line with the latest enhancements. The following table lists new and modified features we documented in the Configuration, Command Reference, and Hardware Installation guides. For information on additional features and fixes that were committed to the SD-WAN solution, see the Resolved and Open Bugs section in the Release Notes.

Table 1: What's New for Cisco vEdge Device

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Getting Started</strong></td>
<td></td>
</tr>
<tr>
<td>API Cross-Site Request Forgery Prevention</td>
<td>This release adds protection against Cross-Site Request Forgery (CSRF) that can occur when you use the SD-WAN REST APIs. This protection is provided by requiring that a CSRF token be included with API requests. You can whitelist requests so that they do not require protection, if needed. For related information, see Cross-Site Request Forgery Prevention.</td>
</tr>
<tr>
<td><strong>Systems and Interfaces</strong></td>
<td></td>
</tr>
<tr>
<td>Secure Shell Authentication Using RSA Keys</td>
<td>This feature enables secure shell authentication between a client and a Cisco SD-WAN server using RSA keys. For related information, see SSH Authentication using vManage on Cisco XE SD-WAN Devices.</td>
</tr>
<tr>
<td><strong>Policies</strong></td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Packet Duplication for Noisy Channels</td>
<td>This feature helps mitigate packet loss over noisy channels, thereby maintaining high application QoE for voice and video. This feature is supported on Cisco XE SD-WAN devices as well as on Cisco vEdge devices. For related information, see Configure and Monitor Packet Duplication.</td>
</tr>
<tr>
<td>Control Traffic Flow Using Class of Service Values</td>
<td>This feature lets you control the flow of traffic into and out of a Cisco vEdge device's interface based on the conditions defined in the quality of service (QoS) map. A priority field and a layer 2 class of service (CoS) were added for configuring the re-write rule. For related information, see Configure Localized Data Policy for IPv4 vManage.</td>
</tr>
<tr>
<td>Security</td>
<td></td>
</tr>
<tr>
<td>IPSec Pairwise Keys</td>
<td>This feature enables support to create and install private pairwise IPSec session keys to secure communication between IPSec devices and its peers. For related information, see IPSec Pairwise Keys Overview.</td>
</tr>
<tr>
<td>Network Optimization and High Availability</td>
<td></td>
</tr>
<tr>
<td>Disaster Recovery for vManage</td>
<td>This feature helps you configure vManage in an active or standby mode to counteract hardware or software failures that may occur due to unforeseen circumstances. For detailed information, see Configure Disaster Recovery.</td>
</tr>
<tr>
<td>Share VNF Devices Across Service Chains</td>
<td>This feature lets you share Virtual Network Function (VNF) devices across service chains to improve resource utilisation and reduce resource fragmentation. For related information, see Share VNF Devices Across Service Chains.</td>
</tr>
<tr>
<td>Monitor Service Chain Health</td>
<td>This feature lets you configure periodic checks on the service chain data path and reports the overall status. To enable service chain health monitoring, NFVIS version 3.12.1 or later should be installed on all CSP devices in a cluster. For related information, see Monitor Service Chain Health.</td>
</tr>
<tr>
<td>Manage PNF Devices in Service Chains</td>
<td>This feature lets you add Physical Network Function (PNF) devices to a network, in addition to the Virtual Network function (VNF) devices. These PNF devices can be added to service chains and shared across service chains, service groups, and a cluster. Inclusion of PNF devices in the service chain can overcome the performance and scaling issues caused by using only VNF devices in a service chain. For related information, see Manage PNF Devices in Service Chains.</td>
</tr>
</tbody>
</table>
Policy Basics

- Policy Overview, on page 3
- Policies in Cisco vManage, on page 5

Policy Overview

Policy influences the flow of data traffic and routing information among Cisco vEdge devices and Cisco XE SD-WAN devices in the overlay network. Policy comprises:

- Routing policy—which affects the flow of routing information in the network's control plane
- Data policy—which affects the flow of data traffic in the network's data plane

To implement enterprise-specific traffic control requirements, you create basic policies, and you deploy advanced features of the Cisco SD-WAN software that are activated by means of the policy configuration infrastructure.

Just as the Cisco SD-WAN overlay network architecture clearly separates the control plane from the data plane and clearly separates control between centralized and localized functions, the Cisco SD-WAN policy software is cleanly separated. Policies apply either to control plane or data plane traffic, and they are configured either centrally (on Cisco vSmart Controllers) or locally (on Cisco vEdge devices and Cisco XE SD-WAN devices). The following figure illustrates the division between control and data policy, and between centralized and local policy.
Control and Data Policy

Control policy is the equivalent of routing protocol policy, and data policy is equivalent to what are commonly called access control lists (ACLs) and firewall filters.

Centralized and Localized Policy

The Cisco SD-WAN policy software design provides a clear separation between centralized and localized policy. In short, centralized policy is provisioned on the centralized Cisco vSmart Controllers in the overlay network, and the localized policy is provisioned on Cisco vEdge devices and Cisco XE SD-WAN devices, which sit at the network edge between a branch or enterprise site and a transport network, such as the Internet, MPLS, or metro Ethernet.

Centralized Policy

Centralized policy refers to policy provisioned on Cisco vSmart Controllers, which are the centralized controllers in the Cisco SD-WAN overlay network. Centralized policy comprises two components:

• Control policy, which affects the overlay network-wide routing of traffic
• Data policy, which affects the data traffic flow throughout the VPN segments in the network

Centralized control policy applies to the network-wide routing of traffic by affecting the information that is stored in the Cisco vSmart Controller’s route table and that is advertised to the Cisco vEdge devices and the Cisco XE SD-WAN devices. The effects of centralized control policy are seen in how Cisco vEdge devices and Cisco XE SD-WAN devices direct the overlay network’s data traffic to its destination.

Note

The centralized control policy configuration itself remains on the Cisco vSmart Controller and is never pushed to local devices.

Centralized data policy applies to the flow of data traffic throughout the VPNs in the overlay network. These policies can permit and restrict access based either on a 6-tuple match (source and destination IP addresses and ports, DSCP fields, and protocol) or on VPN membership.

Note

These policies are pushed to the selected Cisco vEdge devices and the Cisco XE SD-WAN devices.

Localized Policy

Localized policy refers to a policy that is provisioned locally through the CLI on the Cisco vEdge devices and the Cisco XE SD-WAN devices, or through a Cisco vManage device template.

Localized control policy is also called as route policy, which affects (BGP and OSPF) routing behavior on the site-local network.

Localized data policy allows you to provision access lists and apply them to a specific interface or interfaces on the device. Simple access lists permit and restrict access based on a 6-tuple match (source and destination IP addresses and ports, DSCP fields, and protocol), in the same way as with centralized data policy. Access lists also allow provisioning of class of service (CoS), policing, and mirroring, which control how data traffic flows out of and in to the device’s interfaces and interface queues.
The design of the Cisco SD-WAN policy software distinguishes between basic and advanced policy. Basic policy allows you to influence or determine basic traffic flow through the overlay network. Here, you perform standard policy tasks, such as managing the paths along which traffic is routed through the network, and permitting or blocking traffic based on the address, port, and DSCP fields in the packet's IP header. You can also control the flow of data traffic into and out of a Cisco vEdge device's or a Cisco XE SD-WAN device's interfaces, enabling features such as class of service, queuing, and policing. Mirroring is available for Cisco vEdge devices.

Advanced features of Cisco SD-WAN policy software offer specialized policy-based network applications. Examples of these applications include the following:

- Service chaining, which redirects data traffic to shared devices in the network, such as firewall, intrusion detection and prevention (IDS), load balancer, and other devices, before the traffic is delivered to its destination. Service chaining obviates the need to have a separate device at each branch site.

- Application-aware routing, which selects the best path for traffic based on real-time network and path performance characteristics.

- Cflowd, for monitoring traffic flow.

- Converting a Cisco vEdge device into a NAT device, to allow traffic destined for the Internet or other public network can exit directly from the Cisco vEdge device.

By default, no policy of any kind is configured on Cisco XE SD-WAN devices, either on the centralized Cisco vSmart Controllers or the local Cisco vEdge devices and the Cisco XE SD-WAN devices. When control plane traffic, which distributes route information, is unpolicied:

- All route information that OMP propagates among the Cisco XE SD-WAN devices is shared, unmodified, among all Cisco vSmart Controllers and all Cisco vEdge devices and Cisco XE SD-WAN devices in the overlay network domain.

- No BGP or OSPF route policies are in place to affect the route information that Cisco vEdge devices and Cisco XE SD-WAN devices propagate within their local site network.

When data plane traffic is unpolicied, all data traffic is directed towards its destination based solely on the entries in the local Cisco vEdge device and the Cisco XE SD-WAN device's route table, and all VPNs in the overlay network can exchange data traffic.

This section examines the structural components of routing and data policy in the Cisco SD-WAN overlay network.

**Policies in Cisco vManage**

Use the Policies screen to create and activate centralized and localized control and data policies for Cisco vSmart Controllers, Cisco vEdge devices, and Cisco XE SD-WAN devices.

**Screen Elements**

- Top bar—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.

- Title bar—Includes the title of the screen, Policies, and the following:
• Custom Options—Click to display, create, and edit a components for use in policy. For centralized policy, the components are CLI policies, lists, topologies, and traffic policies. For localized policy, the components are CLI policies, lists, forwarding class/QoS definitions, access control lists (ACLs), and route policies.

• Centralized Policy tab—Create a centralized policy. When you first open the Policies screen, the Centralized Policy tab is selected.
  • Add Policy—Click to create a centralized policy using a policy configuration wizard.

• Localized Policy tab—Create a localized policy.
  • Add Policy—Click to create a localized policy using a policy configuration wizard.

• Search box—Includes the Search Options drop-down, for a Contains or Match string.

• Refresh icon—Click to refresh data in the policies table with the most current data.

• Show Table Columns icon—Click to display or hide columns from the policies table. By default, all columns are displayed.

• Policies table—To re-arrange the columns, drag the column title to the desired position.

Configure Policies
  • Configure Centralized Policy
  • Configure Localized Policy
View a Policy

1. In the Centralized Policy or Localized Policy tab, select a policy.
2. Click the More Actions icon to the right of the column and click View. Policies created with the UI policy builder are displayed in graphical format. Policies created using the CLI are displayed in text format.
3. Click Cancel to return to the policies table.

For a policy created using the vManage policy configuration wizard, you can view the policy in text format:

1. In the Centralized Policy or Localized Policy tab, select a policy.
2. Click the More Actions icon to the right of the column and click Preview.
3. Click Cancel to return to the policies table.

Copy a Policy

1. In the Centralized Policy or Localized Policy tab, select a policy.
2. Click the More Actions icon to the right of the column and click Copy.
3. In the Policy Copy popup window, enter the policy name and a description of the policy.

Note

If you are upgrading to 18.4.4, Data Policy names need to be under 26 characters.

Note

Staring Cisco SD-WAN release 19.3, the 127 characters are supported for policy names for the following policy types:
- Central route policy
- Local route policy
- Local Access Control (ACL)
- Local IPv6 ACL
- Central Data Policy
- Central App route policy
- QoS Map
- Rewrite Rule

All other policy names support 32 characters.

4. Click Copy.

Edit a Policy

For policies created using the vManage policy configuration wizard:
1. In the Centralized Policy or Localized Policy tab, select a policy.
2. Click the More Actions icon to the right of the column and click Edit.
3. Edit the policy as needed.
4. Click Save Policy Changes.

For polices created using the CLI:
1. In the Custom Options drop-down, click CLI Policy.
2. Click the More Actions icon to the right of the column and click Edit.
3. Edit the policy as needed.
4. Click Update.

Edit or Create a Policy Component
You can create individual policy components directly and then use them or import them when you are using the policy configuration wizard:

For centralized policy, select the policy component:

- CLI policy—Create the policy using the command-line interface rather than the policy configuration wizard.
- Lists—Create groups of interest to import in the Group of Interest screen in the policy configuration wizard.
- Topology—Create a hub-and-spoke, mesh, or custom topology or a VPN membership to import in the Topology screen in the policy configuration wizard.
- Traffic Policy—Create an application-aware routing, traffic data, or cflowd policy to import in the Traffic Rules screen in the policy configuration wizard.

1. For localized policy, select the policy component:

- CLI policy—Create the policy using the command-line interface rather than the policy configuration wizard.
- Lists—Create groups of interest to import in the Group of Interest screen in the policy configuration wizard.
- Forwarding Class/QoS—Create QoS mappings and rewrite rules to import in the Forwarding Classes/QoS screen in the policy configuration wizard.
- Access Control Lists—Create ACLs of interest to import in the Configure Access Lists screen in the policy configuration wizard.
- Route Policy—Create route policies to import in the Configure Route Policies screen in the policy configuration wizard.
**Delete a Policy**

1. In the Centralized Policy or Localized Policy tab, select a policy.
2. Click the **More Actions** icon to the right of the column and click **Delete**.
3. Click **OK** to confirm deletion of the policy.

**Activate a Centralized Policy on Cisco vSmart Controllers**

1. In the Centralized Policy tab, select a policy.
2. Click the **More Actions** icon to the right of the column and click **Activate**.
3. In the Activate Policy popup, click **Activate** to push the policy to all reachable Cisco vSmart Controllers in the network.
4. Click **OK** to confirm activation of the policy on all Cisco vSmart Controllers.

**Deactivate a Centralized Policy on Cisco vSmart Controllers**

1. In the Centralized Policy tab, select a policy.
2. Click the **More Actions** icon to the right of the column and click **Deactivate**.
3. In the Deactivate Policy popup, click **Deactivate** to confirm that you want to remove the policy from all reachable Cisco vSmart Controllers.
CHAPTER 3

Cisco SD-WAN Policy Framework Basics

This topic offers an orientation about the architecture of the Cisco SD-WAN policy software used to implement overlay network-wide policies. These policies are called vSmart policy or centralized policy, because you configure them centrally on a Cisco vSmart Controller. Cisco vSmart policy affects the flow of both control plane traffic (routing updates carried by Overlay Management Protocol (OMP) and used by the Cisco vSmart Controllers to determine the topology and status of the overlay network) and data plane traffic (data traffic that travels between the Cisco vEdge devices and the Cisco XE SD-WAN devices across the overlay network).

With the Cisco SD-WAN software, you can also create routing policies on the Cisco vEdge devices and the Cisco XE SD-WAN devices. These policies are simply traditional routing policies that are associated with routing protocol (BGP or OSPF) locally on the devices. You use them in the traditional sense for controlling BGP and OSPF, for example, to affect the exchange of route information, to set route attributes, and to influence path selection.

• Cisco vSmart Policy Architecture Components, on page 11
• Cisco vSmart Policy Operation, on page 12
• Configure and Execute Cisco vSmart Policies, on page 16
• Cisco vSmart Policy Components, on page 17
• TLOC Attributes Used in Policies, on page 19
• vRoute Attributes Used in Policies, on page 20
• Cisco vSmart Policy Processing and Application, on page 21

Cisco vSmart Policy Architecture Components

The Cisco vSmart policies that implement overlay network-wide policies are implemented on a Cisco vSmart Controller. Because Cisco vSmart Controllers are centralized devices, you can manage and maintain Cisco vSmart policies centrally, and you can ensure consistency in the enforcement of policy across the overlay network.

The implementation of Cisco vSmart policy is done by configuring the entire policy on the Cisco vSmart Controller. Cisco vSmart policy configuration is accomplished with three building blocks:

• Lists define the targets of policy application or matching.

• Policy definition, or policies, controls aspects of control and forwarding. There are different types of policy, including:
  • app-route-policy (for application-aware routing)
  • cflowd-template (for cflowd flow monitoring)
- control-policy (for routing and control plane information)
- data-policy (for data traffic)
- vpn-membership-policy (for limiting the scope of traffic to specific VPNs)

- Policy application controls what a policy is applied towards. Policy application is site-oriented, and is defined by a specific list called a site-list.

You assemble these three building blocks to Cisco vSmart policy. More specifically, policy is the sum of one or more lists, one policy definition, and at least one policy application, as shown in the table below.

**Table 2: The Three Building Blocks of Cisco vSmart Policy**

<table>
<thead>
<tr>
<th>Lists</th>
<th>Policy Definition</th>
<th>Policy Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>data-prefix-list: List of prefixes for use with a data-policy</td>
<td>app-route-policy: Used with sla-classes for application-aware routing</td>
<td>+ apply-policy: Used with a site-list to determine where policies are applied</td>
</tr>
<tr>
<td>prefix-list: List of prefixes for use with any other policy</td>
<td>cflowd-template: Configures the cflowd agents on the Cisco devices</td>
<td></td>
</tr>
<tr>
<td>site-list: List of site-id:s for use in policy and apply-policy</td>
<td>control-policy: Controls OMP routing control</td>
<td></td>
</tr>
<tr>
<td>tloc-list: List of tloc:s for use in policy</td>
<td>data-policy: Provides vpn-wide policy-based routing</td>
<td></td>
</tr>
<tr>
<td>vpn-list: List of vpn:s for use in policy</td>
<td>vpn-membership-policy: Controls vpn membership across nodes</td>
<td></td>
</tr>
</tbody>
</table>

Complete policy definition configured on Cisco vSmart and enforced either on Cisco vSmart or on Cisco vEdge devices and Cisco XE SD-WAN devices.

**Cisco vSmart Policy Operation**

The basic Cisco vSmart policies are:
- Control Policy
- Data Policy
- VPN Membership

At a high level, control policy operates on routing information, which in the Cisco SD-WAN network is carried in OMP updates. Data policy affects data traffic, and VPN membership controls the distribution of VPN routing tables.
Control Policy Operation

The Cisco SD-WAN devices periodically exchange OMP updates, which carry routing information pertaining to the overlay network. Two of the things that these updates contain are vRoute attributes and Transport Locations (TLOC) attributes.

The Cisco vSmart Controller uses these attributes from the OMP updates to determine the topology and status of the overlay network, and installs routing information about the overlay network into its route table. The controller then advertises the overlay topology to the Cisco vEdge devices and the Cisco XE SD-WAN devices in the network by sending OMP updates to them.

Control policy examines the vRoute and TLOC attributes carried in OMP updates and can modify attributes that match the policy. Any changes that result from control policy are applied directionally, either inbound or outbound.

The figure below shows a control-policy named `prefer_local` that is configured on a Cisco vSmart Controller and that is applied to Site 1 (via site-list list1) and to Site 2 (via site-list list2).

The upper left arrow shows the policy being applied to Site 1—more specifically, to `site-list list1`, which contains an entry for Site 1. The command to apply the policy is `control-policy prefer_local in`. The `in` keyword indicates an inbound policy: the policy is applied to OMP updates that are coming in to the Cisco vSmart Controller from the Cisco vEdge device or the Cisco XE SD-WAN device, which is inbound from the perspective of the controller. So, for all OMP updates that the Site 1 devices sends to the Cisco vSmart Controller, the "prefer_local" control policy is applied before the updates reach the route table on the Cisco vSmart Controller. If any vRoute or TLOC attributes in an OMP update match the policy, any changes that result from the policy actions occur before the Cisco vSmart Controller installs the OMP update information into its route table.
It is important to understand the effect of an inbound policy, because the route table on the Cisco vSmart Controller is used to determine the topology of the overlay network. The Cisco vSmart Controller then distributes this topology information, again via OMP updates, to all the Cisco devices in the network. Because applying policy in the inbound direction influences the information available to the Cisco vSmart Controller to determine the network topology and network reachability, modifying vRoute and TLOC attributes before they are placed in the controller’s route table can provide broad influence over the flow of traffic throughout the overlay network.

On the right side of the figure above, we use the same "prefer_local" policy, but here apply it to Site 2 via the control-policy prefer_local out command. The out keyword in the command indicates an outbound policy, which means that the policy is applied to OMP updates that the Cisco vSmart Controller is sending to the Cisco devices at Site 2. Any changes that result from the policy occur outbound, after the information from the Cisco vSmart Controller's route table has been placed into an OMP update and before the Cisco devices receive the update. Again, note that the direction is outbound from the perspective of the Cisco vSmart Controller.

In contrast to an inbound policy, which affects the centralized route table on the Cisco vSmart Controller and thus can have a broad effect on the route attributes advertised to all the Cisco devices in the overlay network, a control policy applied in the outbound direction influences only the route tables on the individual Cisco devices included in the site-list, so it generally has a more limited scope.

We point out again that in this figure, we are applying the same control policy (the prefer_local policy) to both the inbound and outbound OMP updates. However, the affects of applying the same policy inbound and outbound will be different. The usage shown in the figure illustrates the flexibility of the Cisco SD-WAN control policy design architecture and configuration.

Data Policy Operation

Data policy examines fields in the headers of data packets, looking at the source and destination addresses and ports, and the protocol and DSCP values, and for matching packets, it can modify the next hop in a variety of ways or apply a policer to the packets. Data policy is configured and applied on the Cisco vSmart Controller, and then it is carried in OMP updates to the Cisco XE SD-WAN devices and Cisco vEdge devices in the site-list that the policy is applied to. The match operation and any resultant actions are performed on the Cisco devices as it transmits or receives data traffic.

In the figure below, a data policy named “change_next_hop” is applied to a list of sites that includes Site 3. The OMP update that the vSmart controller sends to the Cisco devices at Site 3 includes this policy definition. When the Cisco device sends or receives data traffic that matches the policy, it changes the next hop to the specified TLOC. Nonmatching traffic is forwarded to the original next-hop TLOC.
In the apply-policy command for a data policy, you specify a direction from the perspective of the Cisco device. In the figure, the "all" direction applies the policy to data traffic transiting the tunnel interface, both what the Cisco device is sending and what it is receiving. You can limit the span of the policy to only incoming traffic (with a data-policy change_next_hop from-tunnel command) or to only outgoing traffic (with a data-policy change_next_hop from-service command).

VPN Membership Policy Operation

VPN membership policy, as the name implies, affects the VPN route tables that are distributed to particular Cisco devices. In an overlay network with no VPN membership policy, the Cisco vSmart Controller pushes the routes for all VPNs to all Cisco devices. If your business usage model restricts participation of specific Cisco devices in particular VPNs, a VPN membership policy is used to enforce this restriction.

The figure below illustrate how VPN membership policy works. This topology has three Cisco devices:

- The Cisco devices at Sites 1 and 2 service only VPN 2.
- The Cisco devices at Site 3 services both VPN 1 and VPN 2.

So here, we want the device at Site 3 to receive all route updates from the Cisco vSmart Controller, because these updates are for both VPN 1 and VPN 2. However, because the other two drivers service only VPN 2, we can filter the route updates sent to them, removing the routes associated with VPN 1 and sending only the ones that apply to VPN 2.
Notice that here, also, you do not set a direction when applying VPN membership policy. This Cisco vSmart Controller always applies this type of policy to the OMP updates that it sends outwards to the Cisco devices.

Configure and Execute Cisco vSmart Policies

All Cisco vSmart Controller policies are configured on the Cisco vSmart Controller, using a combination of policy definition and lists. All Cisco vSmart Controller policies are also applied on the Cisco vSmart Controller, with a combination of apply-policy and lists. However, where the actual Cisco vSmart Controller policy executes depends on the type of policy, as shown in this figure:
For control policy and VPN membership policy, the entire policy configuration remains on the Cisco vSmart Controller, and the actions taken as a result of routes or VPNs that match a policy are performed on the Cisco vSmart Controller.

For the other three policy types—application-aware routing, cflowd templates, and data policy—the policies themselves are transmitted in OMP updates to the Cisco vEdge devices and the Cisco XE SD-WAN devices, and any actions taken as a result of the policies are performed on the Cisco devices.

Cisco vSmart Policy Components

Lists

Lists are how you group related items so that you can reference them all together. Examples of items you put in lists are prefixes, TLOCs, VPNs, and overlay network sites. In the Cisco vSmart Controller policy, you invoke lists in two places: when you create a policy definition and when you apply a policy. Separating the definition of the related items from the definition of policy means that when you can add or remove items from a lists, you make the changes only in a single place: You do not have to make the changes through the policy definition. So if you add ten sites to your network and you want to apply an existing policy to them, you simply add the site identifiers to the site list. You can also change policy rules without having to manually modify the prefixes, VPNs, or other things that the rules apply to.

The following configuration shows the types of Cisco vSmart Controller policy lists:

```
policy
  lists
    data-prefix-list appl1
      ip-prefix 209.165.200.225/27 port 100
    !
    prefix-list pfx1
      ip-prefix 209.165.200.225/27
    !
    site-list sitel
      site-id 100
    !
    tloc-list sitel-tloc
      tloc 209.165.200.225 color mpls
    vpn-list vpn1
  vpn1
```
data-prefix-list is used in data-policy to define prefix and upper layer ports, either individually or jointly, for traffic matching.

prefix-list is used in control-policy to define prefixes for matching RIB entries.

site-list is used in control-policy to match source sites, and in apply-policy to define sites for policy application.

tloc-list is used in control-policy to define TLOCs for matching RIB entries and to apply redefined TLOCs to vRoutes.

vpn-list is used in control-policy to define prefixes for matching RIB entries, and in data-policy and app-route-policy to define VPNs for policy application.

Policy Definition
The policy definition is where you create the policy rules. You specify match conditions (route-related properties for control policy and data-related fields for data policy) and actions to perform when a match occurs. A policy contains match–action pairings that are numbered and that are examined in sequential order. When a match occurs, the action is performed, and the policy analysis on that route or packet terminates. Some types of policy definitions apply only to specific VPNs.

The following configuration shows the components of the Cisco vSmart Controller policy definition. These items are listed in the logical order you should use when designing policy, and this order is also how the items are displayed in the configuration, regardless of the order in which you add them to the configuration.

```
policy
    policy-type name
    vpn-list vpn-list
    sequence number
    match
        <route | tloc vpn | other>
    !
    action <accept reject drop>
    set attribute value
    !
    default-action <reject accept>
    !
```

policy-type—which can be control-policy, data-policy, or vpn-membership (as well as a few other keywords that we discuss later)—dictates the type of policy. Each type has a particular syntax and a particular set of match conditions and settable actions.

vpn-list is used by data-policy and app-route-policy to list the VPNs for which the policy is applicable.

sequence defines each sequential step of the policy by sequence number.

match decides what entity to match on in the specific policy sequence.

action determines the action that corresponds to the preceding match statement.

default-action is the action to take for any entity that is not matched in any sequence of the policy. By default, the action is set to reject.

Policy Application
For a policy definition to take effect, you associate it with sites in the overlay network.
apply-policy
  site-list name
    control-policy name <inout>
  !
  site-list name
  data-policy name
  vpn-membership name
  !

The following are the configuration components:

site-list determines the sites to which a given policy is applies. The direction (in | out) applies only to control-policy.

The policy type—control-policy, data-policy, vpn-membership—and name refer to an already configured policy to be applied to the sites specified in the site-list for the section.

Policy Example

Now, let's put together a complete policy, which consists of lists, policy definition, and policy application. The example illustrated below creates two lists (a site-list and a tloc-list), defines one policy (a control policy), and applies the policy to the site-list. In the figure, the items are listed as they are presented in the node configuration. In a normal configuration process, you create lists first (group together all the things you want to use), then define the policy itself (define what things you want to do), and finally apply the policy (specify the sites that the configured policy affects).

apply-policy
  site-list site1  Apply the defined policy towards the sites in site-list
    control-policy prefer_local out
  !
policy
lists
site-list site1
  site-id 100
tloc-list prefer_site1  Define the lists required for apply-policy and for use within the policy
tloc 192.0.2.1 color mols encap ipsec preference 400
control-policy prefer_local
  sequence 10
    match route
    site-list sitele  Lists previously defined used within policy
      !
    action accept
      set
      tloc-list prefer_site
    !

TLOC Attributes Used in Policies

A transport location, or TLOC, defines a specific interface in the overlay network. Each TLOC consists of a set of attributes that are exchanged in OMP updates among the Cisco SD-WAN devices. Each TLOC is uniquely identified by a 3-tuple of IP address, color, and encapsulation. Other attributes can be associated with a TLOC.

The TLOC attributes listed below can be matched or set in Cisco vSmart Controller policies.
### Table 3:

<table>
<thead>
<tr>
<th>TLOC Attribute</th>
<th>Function</th>
<th>Application Point Set By</th>
<th>Application Point Modify By</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address (IP address)</td>
<td>system-ip address of the source device on which the interface is located.</td>
<td>Configuration on source device</td>
<td>control-policy</td>
</tr>
<tr>
<td>Carrier</td>
<td>Identifier of the carrier type. It primarily indicates whether the transport is public or private.</td>
<td>Configuration on source device</td>
<td>control-policy</td>
</tr>
<tr>
<td>Color</td>
<td>Identifier of the TLOC type.</td>
<td>Configuration on source device</td>
<td>control-policy</td>
</tr>
<tr>
<td>Domain ID</td>
<td>Identifier of the overlay network domain.</td>
<td>Configuration on source device</td>
<td>control-policy</td>
</tr>
<tr>
<td>Encapsulation</td>
<td>Tunnel encapsulation, either IPsec or GRE.</td>
<td>Configuration on source device</td>
<td>control-policy</td>
</tr>
<tr>
<td>Originator</td>
<td>system-ip address of originating node.</td>
<td>Configuration on any originator</td>
<td>control-policy</td>
</tr>
<tr>
<td>Preference</td>
<td>OMP path-selection preference. A higher value is a more preferred path.</td>
<td>Configuration on source device</td>
<td>control-policy</td>
</tr>
<tr>
<td>Site ID</td>
<td>Identification for a give site. A site can have multiple nodes or TLOCs.</td>
<td>Configuration on source device</td>
<td>control-policy</td>
</tr>
<tr>
<td>Tag</td>
<td>Identifier of TLOC on any arbitrary basis.</td>
<td>Configuration on source device</td>
<td>control-policy</td>
</tr>
</tbody>
</table>

### vRoute Attributes Used in Policies

A Cisco SD-WAN route, or vRoute, defines a route in the overlay network. A vRoute, which is similar to a standard IP route, has a number attributes such as TLOC and VPN. The Cisco SD-WAN devices exchange vRoutes in OMP updates.

The vRoutes attributes listed below can be matched or set in Cisco vSmart Controller policies.

### Table 4:

<table>
<thead>
<tr>
<th>vRoute Attribute</th>
<th>Function</th>
<th>Application Point Set By</th>
<th>Application Point Modify By</th>
</tr>
</thead>
<tbody>
<tr>
<td>Origin</td>
<td>Source of the route, either BGP, OSPF, connected, static.</td>
<td>Source device</td>
<td>control-policy</td>
</tr>
</tbody>
</table>
### Cisco vSmart Policy Processing and Application

Understanding how a Cisco vSmart Controller policy is processed and applied allows for proper design of policy and evaluation of how policy is being implemented across the overlay network.

Policy is processed in this way:

- A policy definition consists of a numbered, ordered sequence of match–action pairings. Within each policy, the pairings are processed in sequential order, starting with the lowest number and incrementing.

- As soon as a match occurs, the matched entity is subject to the configured action of the sequence and is then no longer subject to continued processing.

- Any entity not matched in a sequence is subject to the default action for the policy. By default, this action is reject.

Cisco vSmart Controller policy is applied on a per-site-list basis, so:

- When applying policy to a site-list, you can apply only one of each type of policy. For example, you can have one control-policy and one data-policy, or one control-policy in and one control-policy out. You cannot have two data policies or two outbound control policies.

- Because a site-list is a grouping of many sites, you should be careful about including a site in more than one site-list, and in general, we recommend that you not do this at all. You should take special care when a site-list includes a range of site identifiers, to ensure that there is no overlap. If the same site is part of two site-lists and the same type of policy is applied to both site-lists, the policy behavior will be unpredictable and possibly catastrophic.

<table>
<thead>
<tr>
<th>vRoute Attribute</th>
<th>Function</th>
<th>Application Point Set By</th>
<th>Application Point Modify By</th>
</tr>
</thead>
<tbody>
<tr>
<td>Originator</td>
<td>Source of the update carrying the route.</td>
<td>Any originator</td>
<td>control-policy</td>
</tr>
<tr>
<td>Preference</td>
<td>OMP path-selection preference. A higher value is a more preferred path.</td>
<td>Configuration on source device or policy</td>
<td>control-policy</td>
</tr>
<tr>
<td>Service</td>
<td>Advertised service associated with the vRoute.</td>
<td>Configuration on source device</td>
<td>control-policy</td>
</tr>
<tr>
<td>Site ID</td>
<td>Identifier for a give site. A site can have multiple nodes or TLOCs.</td>
<td>Configuration on source device</td>
<td>control-policy</td>
</tr>
<tr>
<td>Tag</td>
<td>Identification on any arbitrary basis.</td>
<td>Configuration on source device</td>
<td>control-policy</td>
</tr>
<tr>
<td>TLOC</td>
<td>TLOC used as next hop for the vRoute.</td>
<td>Configuration on source device or policy</td>
<td>control-policy data-policy</td>
</tr>
<tr>
<td>VPN</td>
<td>VPN to which the vRoute belongs.</td>
<td>Configuration on source device or policy</td>
<td>control-policy data-policy</td>
</tr>
</tbody>
</table>
Control-policy is unidirectional, being applied either inbound to the vSmart controller or outbound from it. When control-policy is needed in both directions, configure two control policies. Data-policy is bidirectional and can be applied either to traffic received from the service side of the Cisco vEdge device or the Cisco XE SD-WAN device, traffic received from the tunnel side, or all of these combinations. VPN membership policy is always applied to traffic outbound from the Cisco vSmart Controller.

Control-policy remains on the Cisco vSmart Controller and affects routes that the controller sends and receives. Data-policy is sent to either the Cisco vEdge devices or the Cisco XE SD-WAN devices in the site-list. The policy is sent in OMP updates, and it affects the data traffic that the devices send and receive.

When any node in the overlay network makes a routing decision, it uses any and all available routing information. In the overlay network, it is the Cisco vSmart Controller that distributes routing information to the Cisco device nodes. In a network deployment that has two or more Cisco vSmart Controllers, each controller acts independently to disseminate routing information to other Cisco vSmart Controllers and to Cisco XE SD-WAN devices and Cisco vEdge devices in the overlay network. So, to ensure that the Cisco vSmart Controller policy has the desired effect in the overlay network, each Cisco vSmart Controller must be configured with the same policy, and the policy must be applied identically. What this means is that for any given policy, you must configure the identical policy and apply it identically across all the Cisco vSmart Controllers.
Control Policies

Control policy, which is similar to standard routing policy, operates on routes and routing information in the control plane of the overlay network. Centralized control policy, which is provisioned on the Cisco vSmart Controller, is the Cisco SD-WAN technique for customizing network-wide routing decisions that determine or influence routing paths through the overlay network. Local control policy, which is provisioned on a Cisco vEdge device or a Cisco XE SD-WAN device, allows customization of routing decisions made by BGP and OSPF on site-local branch or enterprise networks.

The routing information that forms the basis of centralized control policy is carried in Cisco SD-WAN route advertisements, which are transmitted on the DTLS or TLS control connections between Cisco vSmart Controllers and Cisco vEdge devices or Cisco XE SD-WAN devices. Centralized control policy determines which routes and route information are placed into the centralized route table on the Cisco vSmart Controller and which routes and route information are advertised to the Cisco devices in the overlay network. Basic centralized control policy establish traffic engineering, to set the path that traffic takes through the network. Advanced control policy supports a number of features, including service chaining, which allows Cisco devices in the overlay network to share network services, such as firewalls and load balancers.

Centralized control policy affects the OMP routes that are distributed by the Cisco vSmart Controller throughout the overlay network. The Cisco vSmart Controller learns the overlay network topology from OMP routes that are advertised by the Cisco devices over the OMP sessions inside the DTLS or TLS connections between the Cisco vSmart Controller and the drivers. (The DTLS connections are shown in orange in the figure to the right).

Three types of OMP routes carry the information that the Cisco vSmart Controller uses to determine the network topology:

- Cisco SD-WAN OMP routes, which are similar to IP route advertisements, advertise routing information that Cisco devices have learned from their local site and the local routing protocols (BGP and OSPF) to the Cisco vSmart Controller. These routes are also referred to as OMP routes or vRoutes.
• TLOC routes carry overlay network–specific locator properties, including the IP address of the interface that connects to the transport network, a link color, which identifies a traffic flow, and the encapsulation type. (A TLOC, or transport location, is the physical location where a Cisco device connects to a transport network. It is identified primarily by IP address, link color, and encapsulation, but a number of other properties are associated with a TLOC.)

• Service routes advertise the network services, such as firewalls, available to VPN members at the Cisco device's local site.

By default, no centralized control policy is provisioned. In this bare, unpolicyed network, all OMP routes are placed in the Cisco vSmart Controller's route table as is, and the Cisco vSmart Controller advertised all OMP routes, as is, to all Cisco devices in the same VPN in the network domain.

By provisioning centralized control policy, you can affect which OMP routes are placed in the Cisco vSmart Controller's route table, what route information is advertised to the Cisco devices, and whether the OMP routes are modified before being put into the route table or before being advertised.

Cisco devices place all the route information learned from the Cisco vSmart Controllers, as is, into their local route tables, for use when forwarding data traffic. Because the Cisco vSmart Controller's role is to be the centralized routing system in the network, Cisco devices can never modify the OMP route information that they learn from the Cisco vSmart Controllers.

The Cisco vSmart Controller regularly receives OMP route advertisements from the Cisco devices and, after recalculating and updating the routing paths through the overlay network, it advertises new routing information to the Cisco devices.

The centralized control policy that you provision on the Cisco vSmart Controller remains on the Cisco vSmart Controller and is never downloaded to the Cisco devices. However, the routing decisions that result from centralized control policy are passed to the Cisco devices in the form of route advertisements, and so the affect of the control policy is reflected in how the Cisco devices direct data traffic to its destination.

A type of centralized control policy called service chaining allows data traffic to be routed through one or more network services, such as firewall, load balancer, and intrusion detection and prevention (IDP) devices, en route to its destination.

Localized control policy, which is provisioned locally on the Cisco devices, is called route policy. This policy is similar to the routing policies that you configure on a regular driver, allowing you to modify the BGP and OSPF routing behavior on the site-local network. Whereas centralized control policy affects the routing behavior across the entire overlay network, route policy applies only to routing at the local branch.

• Centralized Control Policy, on page 25
• Localized Control Policy, on page 58
Centralized Control Policy

In the Cisco SD-WAN network architecture, centralized control policy is handled by the Cisco vSmart Controller, which effectively is the routing engine of the Cisco SD-WAN network. The Cisco vSmart Controller is the centralized manager of network-wide routes, maintaining a master route table for these routes. The Cisco vSmart Controller builds its route table based on the route information advertised by the Cisco vEdge devices and the Cisco XE SD-WAN devices in its domain, using these routes to discover the network topology and to determine the best paths to network destinations. The Cisco vSmart Controller distributes route information from its route table to the Cisco devices in its domain, and the Cisco devices use these routes to forward data traffic through the network. The result of this architecture is that networking-wide routing decisions and routing policy are orchestrated by a central authority instead of being implemented hop by hop, by the devices in the network.

Centralized control policy allows you to influence the network routes advertised by the Cisco vSmart Controllers. This type of policy, which is provisioned centrally on the Cisco vSmart Controller, affects both the route information that the Cisco vSmart Controller stores in its master route table and the route information that it distributes to the Cisco devices.

Centralized control policy is provisioned and applied only on the Cisco vSmart Controller. The control policy configuration itself is never pushed to Cisco devices in the overlay network. What is pushed to the Cisco devices, using the Overlay Management Protocol (OMP), are the results of the control policy, which the Cisco devices then install in their local route tables and use for forwarding data traffic. This design means that the distribution of network-wide routes is always administered centrally, using policies designed by network administrators. These policies are always implemented by centralized Cisco vSmart Controllers, which are responsible for orchestrating the routing decisions in the Cisco SD-WAN overlay network.

Within a network domain, the network topology map on all Cisco vSmart Controllers must be synchronized. To support this, you must configure identical policies on all the Cisco vSmart Controllers in the domain.

All centralized control plane traffic, including route information, is carried by OMP peering sessions that run within the secure, permanent DTLS connections between Cisco devices and the Cisco vSmart Controllers in their domain. The end points of an OMP peering session are identified by the system IDs of the Cisco devices, and the peering sessions carry the site ID, which identifies the site in which the device is located. A DTLS connection and the OMP session running over it remain active as long as the two peers are operational.
Control policy can be applied both inbound, to the route advertisements that the Cisco vSmart Controller receives from the Cisco devices, and outbound, to advertisements that it sends to them. Inbound policy controls which routes and route information are installed in the local routing database on the Cisco vSmart Controller, and whether this information is installed as-is or is modified. Outbound control policy is applied after a route is retrieved from the routing database, but before a Cisco vSmart Controller advertises it, and affects whether the route information is advertised as-is or is modified.

**Configure the Network Topology**

When you first open the Configure Topology and VPN Membership screen, the **Topology** tab is selected by default.

To configure the network topology and VPN membership:

### Hub and Spoke

- **Step 1**: In the Add Topology drop-down, select **Hub and Spoke**.
- **Step 2**: Enter a name for the hub-and-spoke policy.
- **Step 3**: Enter a description for the policy.
- **Step 4**: In the VPN List field, select the VPN list for the policy.
- **Step 5**: In the left pane, click **Add Hub and Spoke**. A hub-and-spoke policy component containing the text string My Hub-and-Spoke is added in the left pane.
- **Step 6**: Double-click the **My Hub-and-Spoke** text string, and enter a name for the policy component.
- **Step 7**: In the right pane, add hub sites to the network topology:
  a) Click **Add Hub Sites**.
  b) In the **Site List Field**, select a site list for the policy component.
  c) Click **Add**.
  d) Repeat these steps to add more hub sites to the policy component.
- **Step 8**: In the right pane, add spoke sites to the network topology:
  a) Click **Add Spoke Sites**.
  b) In the **Site List Field**, select a site list for the policy component.
  c) Click **Add**.
  d) Repeat these steps to add more spoke sites to the policy component.
- **Step 9**: Repeat steps as needed to add more components to the hub-and-spoke policy.
- **Step 10**: Click **Save Hub and Spoke Policy**.

### Mesh

Policy for a topology with a partial-mesh or full-mesh region.

- **Step 1**: In the Add Topology drop-down, select **Mesh**.
- **Step 2**: Enter a name for the mesh region policy component.
- **Step 3**: Enter a description for the mesh region policy component.
### Step 4
In the **VPN List** field, select the VPN list for the policy.

### Step 5
Click **New Mesh Region**.

### Step 6
In the **Mesh Region Name** field, enter a name for the individual mesh region.

### Step 7
In the **Site List** field, select one or more sites to include in the mesh region.

### Step 8
Repeat these steps to add more mesh regions to the policy.

### Step 9
Click **Save Mesh Region**.

---

### Custom Control (Route and TLOC)

Policy for a topology with custom route and TLOC configuration.

### Step 1
In the Add Topology drop-down, select **Custom Control (Route & TLOC)**.

### Step 2
Enter a name for the custom control policy component.

### Step 3
Enter a description of the custom control policy component.

### Step 4
Click **Sequence Type**. The Add Control Policy popup displays.

### Step 5
Click **Route** or **TLOC** to create a policy of that type.

### Step 6
Click **Sequence Rule**.

---

### Custom Control (Route)

Create a policy to apply on an OMP route. By default, the Match tab is selected, displaying match condition options.

### Step 1
From the Add Custom Control Policy screen, click **Route**.

### Step 2
Click **Sequence Rule**. Match and Actions options display.

### Step 3
From the Match tab, select and configure match conditions for your route.

<table>
<thead>
<tr>
<th><strong>Match Condition</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Color List</td>
<td>Select a color list to match, or click <strong>New Color List</strong> to create a new list:</td>
</tr>
<tr>
<td></td>
<td>a. Enter a name for the Color list.</td>
</tr>
<tr>
<td></td>
<td>b. From the <strong>Select Color</strong> drop-down menu, select the color(s) you want included in your list.</td>
</tr>
<tr>
<td></td>
<td>c. Click <strong>Save</strong>.</td>
</tr>
<tr>
<td>OMP Tag</td>
<td>Enter the OMP route tag, a number between 0-4294967295.</td>
</tr>
<tr>
<td>Origin</td>
<td>Select an origin for the route from the drop-down menu. Options include <strong>Aggregate</strong>, <strong>BGP External</strong>, <strong>BGP Internal</strong>, <strong>Connected</strong>, <strong>OSPF Inter-Area</strong>, <strong>OSPF Intra-Area</strong>, <strong>OSPF External 1</strong>, <strong>OSPF External 2</strong>, and <strong>Static</strong>.</td>
</tr>
<tr>
<td>Originator</td>
<td>Enter the IP address of the originator of this route.</td>
</tr>
<tr>
<td>Match Condition</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Preference</td>
<td>Enter the preference number for the route, a number between 0-4294967295.</td>
</tr>
<tr>
<td>Site</td>
<td>Select a site list from the list of options, or create a new site list: a. Enter a name for the Site list. b. Enter the Site numbers, following the example. c. Click Save.</td>
</tr>
<tr>
<td>TLOC</td>
<td>Select a TLOC list to match, or create a new TLOC list: a. Enter a name for the TLOC list. b. In the TLOC IP field, enter the IP address for the TLOC. c. In the Color drop-down menu, select the color you want to apply to the TLOC list. d. From the Encap drop-down menu, select the encapsulation type for the TLOC list. e. In the Preference field, enter the preference number for the route, a number between 0-4294967295. f. Optionally, click Add TLOC and repeat steps 1-5 to open another TLOC list. g. Click Save.</td>
</tr>
<tr>
<td>VPN</td>
<td>a. From the Match Conditions &gt; VPN list field, select a VPN list, or click New VPN List to create a new one: b. Enter a name for the VPN List. c. In the VPN field, enter the VPN numbers, for example, 100 or 200 separated by commas, or 1000-2000 by range. d. Click Save.</td>
</tr>
<tr>
<td>Prefix List</td>
<td>From the Match Conditions &gt; Prefix List field, select a Prefix list, or click New Prefix List to create a new one: a. From the Prefix List drop-down menu, select a prefix list, or create a new one. b. In the Add Prefix field, enter the IP prefixes, or click Import on the right to import prefixes. c. Click Save. Note: The Prefix List option is not available if you select protocol Both (IPv4 and IPv6).</td>
</tr>
</tbody>
</table>

**Step 4** From the Actions tab, select IPv4, IPv6, or Both, to designate which protocol the actions should apply to. Not all of the following options are available for all protocols.

**Step 5** Click Accept or Reject for the IP traffic meeting the match conditions:
<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Conditions</th>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept</td>
<td>Allow traffic from the selected protocol. Click the following menu buttons to open configuration fields:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Export To</td>
<td>Select a VPN list, or create a new one.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OMP Tag</td>
<td>Enter the OMP route tag, a number between 0-4294967295.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Preference</td>
<td>Enter the preference number for the route, a number between 0-4294967295.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service</td>
<td>Enter the following information:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>Select a service type. Options are:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Firewall</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Intrusion Detection Prevention</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Intrusion Detection System</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Net Service 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Net Service 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Net Service 3</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Net Service 4</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Net Service 5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VPN</td>
<td>Enter the number of the Service VPN.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TLOC IP</td>
<td>Enter the IP address of the Service TLOC.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Color</td>
<td>Select a Color type from the drop-down list.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encapsulation</td>
<td>Select IPSEC or GRE as the encapsulation type</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TLOC List</td>
<td>Select a service TLOC list from the drop-down menu, or create a new one.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TLOC Action</td>
<td>Select an action from the drop-down menu.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strict</td>
<td>Direct matching traffic only to the intermediate destination. With this action, if the intermediate destination is down, no traffic reaches the final destination. If you do not configure a set loc-action action in a centralized control policy, strict is the default behavior.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Primary</td>
<td>First direct matching traffic to the intermediate destination. If that driver is not reachable, then direct it to the final destination. With this action, if the intermediate destination is down, all traffic reaches the final destination.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Backup</td>
<td>First direct matching traffic to the final destination. If that driver is not reachable, then direct it to the intermediate destination. With this action, if the source is unable to reach the final destination directly, it is possible for all traffic to reach the final destination via the intermediate destination.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Custom Control (TLOC)

Create a policy to apply to a TLOC. By default, the Match tab is selected, displaying match condition options.

### Step 1
From the Add Custom Control Policy screen, click TLOC.

### Step 2
Click Sequence Rule. Match and Actions options display.

### Step 3
From the Match tab, select and configure match conditions for your route.

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Conditions</th>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Carrier</strong></td>
<td></td>
<td></td>
<td>Select a carrier from the drop-down list.</td>
</tr>
<tr>
<td><strong>Color List</strong></td>
<td></td>
<td></td>
<td>Select a color list from the drop-down list, or create a new one.</td>
</tr>
<tr>
<td><strong>Domain ID</strong></td>
<td></td>
<td></td>
<td>Enter a domain ID number, between 1-4294967295.</td>
</tr>
<tr>
<td><strong>Group ID</strong></td>
<td></td>
<td></td>
<td>Enter a Group ID number, between 1-4294967295.</td>
</tr>
<tr>
<td><strong>OMP Tag</strong></td>
<td></td>
<td></td>
<td>Enter an OMP tag number, between 1-4294967295.</td>
</tr>
<tr>
<td><strong>Originator</strong></td>
<td></td>
<td></td>
<td>Enter the IP address of the originator of the TLOC.</td>
</tr>
<tr>
<td><strong>Preference</strong></td>
<td></td>
<td></td>
<td>Enter a preference number for the policy, between 1-4294967295.</td>
</tr>
</tbody>
</table>

**Equal Cost Multi-path**

Equally direct matching control traffic between the intermediate destination and the ultimate destination. With this action, if the intermediate destination is down, all traffic reaches the ultimate destination.

<table>
<thead>
<tr>
<th>TLOC</th>
<th>Enter the following information:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TLOC List</strong></td>
<td>Select a TLOC list, or create a new one.</td>
</tr>
<tr>
<td><strong>TLOC IP</strong></td>
<td>Enter the IP address of the designated TLOC.</td>
</tr>
<tr>
<td><strong>Color</strong></td>
<td>Select a color from the available options.</td>
</tr>
</tbody>
</table>

**Encapsulation**

Select IPSEC or GRE as the encapsulation type.

**Reject**

Reject traffic for the selected conditions.

a. Select a protocol from the Protocol dropdown: IPv4, IPv6, or Both.

b. Click Accept or Reject for the match conditions.

c. Optionally, repeat these steps with a different protocol.

Click Save Match and Actions.
<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site List</td>
<td>Select a site list from the drop-down list, create a new one, or enter a site ID in the Site ID field, between 1-4294967295.</td>
<td></td>
</tr>
<tr>
<td>TLOC</td>
<td>a. Select a TLOC from the drop-down list, or create a new one.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. Enter the following values:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TLOC IP</td>
<td>Enter the IP address of the TLOC.</td>
</tr>
<tr>
<td></td>
<td>Color</td>
<td>Select a color list from the available options.</td>
</tr>
<tr>
<td></td>
<td>Encapsulation</td>
<td>Select IPSEC or GRE as the encapsulation type.</td>
</tr>
</tbody>
</table>

### Step 4
Click **Accept** or **Reject** to apply the following match conditions to an action.

<table>
<thead>
<tr>
<th>Action Condition</th>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept</td>
<td>Allow traffic from the selected protocol. Click the following menu buttons to open configuration fields:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>OMP Tag</td>
<td>Enter an OMP tag number, between 1-4294967295.</td>
</tr>
<tr>
<td></td>
<td>Preference</td>
<td>Enter a preference number for the policy, between 1-4294967295.</td>
</tr>
<tr>
<td>Reject</td>
<td>Reject traffic for the selected conditions.</td>
<td></td>
</tr>
</tbody>
</table>

---

**Import Existing Topology**

You can select an existing topology to use in your policy.

**Step 1**
In the Add Topology drop-down, select **Import Existing Topology** to open the matching popup.

**Step 2**
Under **Policy Type**, click the topology type you want to import:

- a) **Hub and Spoke**
- b) **Mesh**
- c) **Custom**

**Step 3**
Select a policy from the field list. Cisco vManage populates this field from the available topologies for the type you select.

**Step 4**
Click **Import**.

**Step 5**
Click **Save Control Policy** to save the Route policy.

---

**Create a VPN Membership Policy**

You can create a VPN membership policy for the topology.
Step 1  In the Topology bar, click VPN Membership. Then:
Step 2  Click Add VPN Membership Policy. The Update VPN Membership Policy popup displays.
Step 3  Enter a name and description for the VPN membership policy.
Step 4  In the Site List field, select the site list.
Step 5  In the VPN Lists field, select the VPN list.
Step 6  Click Add List to add another VPN to the VPN membership.
Step 7  Click Save.
Step 8  Click Next to move to Configure Traffic Rules in the wizard.

Route Types

The Cisco vSmart Controller learns the network topology from OMP routes, which are Cisco SD-WAN-specific routes carried by OMP. There are three types of OMP routes:

- Cisco SD-WAN OMP routes—These routes carry prefix information that the Cisco devices learn from the routing protocols running on its local network, including routes learned from BGP and OSPF, as well as direct, connected, and static routes. OMP advertises OMP routes to the Cisco vSmart Controller by means of an OMP route SAFI (Subsequent Address Family Identifier). These routes are commonly simply called OMP routes.

- TLOC routes—These routes carry properties associated with transport locations, which are the physical points at which the Cisco devices connect to the WAN or the transport network. Properties that identify a TLOC include the IP address of the WAN interface and a color that identifies a particular traffic flow. OMP advertises TLOC routes using a TLOC SAFI.

- Service routes—These routes identify network services, such as firewalls and IDPs, that are available on the local-site network to which the Cisco devices are connected. OMP advertises these routes using a service SAFI.

Default Behavior Without Centralized Control Policy

By default, no centralized control policy is provisioned on the Cisco vSmart Controller. This results in the following route advertisement and redistribution behavior within a domain:

- All Cisco vEdge devices and Cisco XE SD-WAN devices redistribute all the route-related prefixes that they learn from their site-local network to the Cisco vSmart Controller. This route information is carried by OMP route advertisements that are sent over the DTLS connection between the Cisco devices and the Cisco vSmart Controller. If a domain contains multiple Cisco vSmart Controllers, the Cisco devices send all OMP route advertisements to all the controllers.

- All Cisco devices send all TLOC routes to the Cisco vSmart Controller or controllers in their domain, using OMP.

- All Cisco devices send all service routes to advertise any network services, such as firewalls and IDPs, that are available at the local site where the Cisco device is located. Again, these are carried by OMP.

- The Cisco vSmart Controller accepts, as is, all the OMP, TLOC, and service routes that it receives from all Cisco devices in its domain, storing the information in its route table. The Cisco vSmart Controller
tracks which OMP routes, TLOCs, and services belong to which VPNs. The Cisco vSmart Controller uses all the routes to develop a topology map of the network and to determine routing paths for data traffic through the overlay network.

- The Cisco vSmart Controller redistributes all information learned from the OMP, TLOC, and service routes in a particular VPN to all Cisco devices in the same VPN.
- The Cisco devices regularly send route updates to the Cisco vSmart Controller.
- The Cisco vSmart Controller recalculates routing paths, updates its route table, and advertises new and changed routing information to all the Cisco devices.

**Behavior Changes with Centralized Control Policy**

When you do not want to redistribute all route information to all Cisco vEdge devices and Cisco XE SD-WAN devices in a domain, or when you want to modify the route information that is stored in the Cisco vSmart Controller's route table or that is advertised by the Cisco vSmart Controller, you design and provision a centralized control policy. To activate the control policy, you apply it to specific sites in the overlay network in either the inbound or the outbound direction. The direction is with respect to the Cisco vSmart Controller. All provisioning of centralized control policy is done on the Cisco vSmart Controller.

Applying a centralized control policy in the inbound direction filters or modifies the routes being advertised by the Cisco vEdge device and the Cisco XE SD-WAN device before they are placed in the route table on the Cisco vSmart Controller. As the first step in the process, routes are either accepted or rejected. Accepted routes are installed in the route table on the Cisco vSmart Controller either as received or as modified by the control policy. Routes that are rejected by a control policy are silently discarded.

Applying a control policy in outbound direction filters or modifies the routes that the Cisco vSmart Controller redistributes to the Cisco vEdge device and the Cisco XE SD-WAN devices. As the first step of an outbound policy, routes are either accepted or rejected. For accepted routes, centralized control policy can modify the routes before they are distributed by the Cisco vSmart Controller. Routes that are rejected by an outbound policy are not advertised.
VPN Membership Policy

A second type of centralized data policy is VPN membership policy. It controls whether a Cisco vEdge device or a Cisco XE SD-WAN device can participate in a particular VPN. Stated another way, VPN membership policy defines which VPNs a Cisco vEdge device or Cisco XE SD-WAN device is and is not allowed to receive routes from.

VPN membership policy can be centralized, because it affects only the packet headers and has no impact on the choice of interface that a Cisco vEdge device or a Cisco XE SD-WAN device uses to transmit traffic. What happens instead is that if, because of a VPN membership policy, a Cisco vEdge device or a Cisco XE SD-WAN device is not allowed to receive routes for a particular VPN, the Cisco vSmart Controller never forwards those routes to that driver.

Examples of Modifying Traffic Flow with Centralized Control Policy

This section provides some basic examples of how you can use centralized control policies to modify the flow of data traffic through the overlay network.

Create an Arbitrary Topology

When data traffic is exchanged between two Cisco devices, if you have provisioned no control policy, the two Cisco devices establish an IPsec tunnel between them and the data traffic flows directly from one device to the next. For a network with only two devices or with just a small number of Cisco devices, establishing connections between each pair of devices is generally not been an issue. However, such a solution does not scale. In a network with hundreds or even thousands of branches, establishing a full mesh of IPsec tunnels would tax the CPU resources of each Cisco device.

One way to minimize this overhead is to create a hub-and-spoke type of topology in which one of the Cisco devices acts as a hub site that receives the data traffic from all the spoke, or branch, devices and then redirects the traffic to the proper destination. This example shows one of the ways to create such a hub-and-spoke
The figure here illustrates how such a policy might work. The topology has two branch locations, West and East. When no control policy is provisioned, these two Cisco devices exchange data traffic with each other directly by creating an IPsec tunnel between them (shown by the red line). Here, the route table on the Device West contains a route to Device East with a destination TLOC of 203.0.113.1, color gold (which we write as the tuple \( \{192.0.2.1, \text{gold}\} \)), and Device East route table has a route to the West branch with a destination TLOC of \( \{203.0.113.1, \text{gold}\} \).

To set up a hub-and-spoke-type topology here, we provision a control policy that causes the West and East devices to send all data packets destined for the other device to the hub device. (Remember that because control policy is always centralized, you provision it on the Cisco vSmart Controller.) On the Device West, the policy simply changes the destination TLOC from \( \{203.0.113.1, \text{gold}\} \) to \( \{209.165.200.225, \text{gold}\} \), which is the TLOC of the hub device, and on the Device East, the policy changes the destination TLOC from \( \{192.0.2.1, \text{gold}\} \) to the hub's TLOC, \( \{209.165.200.225, \text{gold}\} \). If there were other branch sites on the west and east sides of the network that exchange data traffic, you could apply these same two control policies to have them redirect all their data traffic through the hub.

Set Up Traffic Engineering

Control policy allows you to design and provision traffic engineering. In a simple case, suppose that you have two Cisco devices acting as hub devices. Here, you might want data traffic destined to a branch Cisco vEdge device or a Cisco XE SD-WAN device to always transit through one of the hub devices. To engineer this traffic flow, you set the TLOC preference value to favor the desired hub device.

The figure on the left shows that Site ID 100 has two hub devices, one that serves the West side of the network and a second that serves the East side. Data traffic from the Device West must be handled by the Device West hub, and similarly, data traffic from the Device East branch must go through the Device East hub.

To engineer this traffic flow, you provision two control policies, one for Site ID 1, where the Device West device is located, and a second one for Site ID 2. The control policy for Site ID 1 changes the TLOC for traffic destined to the Device East to \( \{209.165.200.225, \text{gold}\} \), and the control policy for Site ID 2 changes the TLOC...
for traffic destined for Site ID 1 to \{198.51.100.1, gold\}. One additional effect of this traffic engineering policy is that it load-balances the traffic traveling through the two hub devices.

With such a traffic engineering policy, a route from the source device to the destination device is installed in the local route table, and traffic is sent to the destination regardless of whether the path between the source and destination devices is available. Enabling end-to-end tracking of the path to the ultimate destination allows the Cisco vSmart Controller to monitor the path from the source to the destination, and to inform the source device when that path is not available. The source device can then modify or remove the path from its route table.

The figure to the right illustrates end-to-end path tracking. It shows that traffic from Device-A that is destined for Device-D first goes to an intermediate device, Device-B, perhaps because this intermediate device provides a service, such as a firewall. (You configure this traffic engineering with a centralized control policy that is applied to Device-A, at Site 1.) Then Device-B, which has a direct path to the ultimate destination, forwards the traffic to Device-D. So, in this example, the end-to-end path between Device-A and Device-D comprises two tunnels, one between Device-A and Device-B, and the second between Device-B and Device-D. The Cisco vSmart Controller tracks this end-to-end path, and it notifies Device-A if the portion of the path between Device-B and Device-D becomes unavailable.

As part of end-to-end path tracking, you can specify how to forwarded traffic from the source to the ultimate destination using an intermediate device. (You do this by setting the TLOC action in the action portion of the control policy.) The default method is strict forwarding, where traffic is always sent from Device-A to Device-B, regardless of whether Device-B has a direct path to Device-D or whether the tunnel between Device-B and Device-D is up. More flexible methods forward some or all traffic directly from Device-A to Device-D. You can also set up a second intermediate device to provide a redundant path with the first intermediate device is unreachable and use an ECMP method to forward traffic between the two. The figure below adds Device-C as a redundant intermediate device.
Centralized control policy, which you configure on Cisco vSmart Controllers, affects routing policy based on information in OMP routes and OMP TLOCs.

This type of policy allows you to set actions for matching routes and TLOCs, including redirecting packets through network services, such as firewalls, a feature that is called service chaining.

In domains with multiple Cisco vSmart Controllers, all the controllers must have the same centralized control policy configuration to ensure that routing within the overlay network remains stable and predictable.

**Configuration Components**

A centralized control policy consists of a series of numbered (ordered) sequences of match-action pairs that are evaluated in order, from lowest sequence number to highest sequence number. When a route or TLOC matches the match conditions, the associated action or actions are taken and policy evaluation on that packets stops. Keep this process in mind as you design your policies to ensure that the desired actions are taken on the items subject to policy.

If a route or TLOC matches no parameters in any of the sequences in the policy configure, it is, by default, rejected and discarded.

The following figure illustrates the configuration components for centralized control policy.
Configure Centralized Policy Using Cisco vManage

To configure centralized policies, use the Cisco vManage policy configuration wizard. The wizard consists of four sequential screens that guide you through the process of creating and editing policy components:

- **Create Groups of Interest**—Create lists that group together related items and that you call in the match or action components of a policy.
- **Configure Topology**—Create the network structure to which the policy applies.
- **Configure Traffic Rules**—Create the match and action conditions of a policy.
- **Apply Policies to Sites and VPNs**—Associate policy with sites and VPNs in the overlay network.

In the first three policy configuration wizard screens, you are creating policy components or blocks. In the last screen, you are applying policy blocks to sites and VPNs in the overlay network.

For a centralized policy to take effect, you must activate the policy.

**Step 1: Start the Policy Configuration Wizard**

To start the policy configuration wizard:

1. In the Cisco vManage NMS, select the **Configure > Policies** screen.
2. Select the **Centralized Policy** tab.
3. Click **Add Policy**.

The policy configuration wizard appears, and the **Create Applications or Groups of Interest** screen is displayed.

**Step 2: Configure Groups of Interest**

In **Create Groups of Interest**, create lists of groups to use in a centralized policy:
1. Create new lists, as described in the following table:

<table>
<thead>
<tr>
<th>List Type</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| Color     | a. In the left bar, click **Color**.  
|           | b. Click **New Color List**.  
|           | c. Enter a name for the list.  
|           | d. From the Select Color drop-down, select the desired colors.  
|           | e. Click **Add**.  |
| Prefix    | a. In the left bar, click **Prefix**.  
|           | b. Click **New Prefix List**.  
|           | c. Enter a name for the list.  
|           | d. In the Add Prefix field, enter one or more data prefixes separated by commas.  
<p>|           | e. Click <strong>Add</strong>.  |</p>
<table>
<thead>
<tr>
<th>List Type</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| Site      | a. In the left bar, click Site.  
b. Click New Site List.  
c. Enter a name for the list.  
d. In the Add Site field, enter one or more site IDs separated by commas.  
e. Click Add. |
| TLOC      | a. In the left bar, click TLOC.  
b. Click New TLOC List. The TLOC List popup displays.  
c. Enter a name for the list.  
d. In the TLOC IP field, enter the system IP address for the TLOC.  
e. In the Color field, select the TLOC’s color.  
f. In the Encap field, select the encapsulation type.  
g. In the Preference field, optionally select a preference to associate with the TLOC.  
h. Click Add TLOC to add another TLOC to the list.  
i. Click Save. |
| VPN       | a. In the left bar, click VPN.  
b. Click New VPN List.  
c. Enter a name for the list.  
d. In the Add VPN field, enter one or more VPN IDs separated by commas.  
e. Click Add. |

2. Click Next to move to Configure Topology and VPN Membership in the wizard.

**Step 3: Configure Topology and VPN Membership**

When you first open the Configure Topology and VPN Membership screen, the Topology tab is selected by default:

To configure topology and VPN membership:

1. In the Topology tab, create a network topology, as described in the following table:
<table>
<thead>
<tr>
<th>Topology Type</th>
<th>Description</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| Custom Control (Route & TLOC) | Centralized route control policy (for matching OMP routes) | 1. In the Add Topology drop-down, select **Custom Control (Route & TLOC)**.  
2. Enter a name for the control policy.  
3. Enter a description for the policy.  
4. In the left pane, click **Add Sequence Type**. The Add Control Policy popup displays.  
5. Select **Route**. A policy component containing the text string Route is added in the left pane.  
6. Double-click the **Route** text string, and enter a name for the policy component.  
7. In the right pane, click **Add Sequence Rule**. The Match/Actions box opens, and Match is selected by default.  
8. From the boxes under the Match box, select the desired policy match type. Then select or enter the value for that match condition. Configure additional match conditions for the sequence rule, as desired. For an explanation of the match conditions, see the OMP Route Match Attributes section in the Configuring Centralized Control Policy topic for your software release.  
9. Click **Actions**. The Reject radio button is selected by default. To configure actions to perform on accepted packets, click the **Accept** radio button. Then select the action or enter a value for the action. For an explanation of the actions, see the Action Parameters section in the Configuring Centralized Control Policy topic for your software release.  
10. Click **Save Match and Actions**.  
11. Click **Add Sequence Rules** to configure more sequence rules, as desired. Drag and drop to re-order them.  
12. Click **Add Sequence Type** to configure more sequences, as desired. Drag and drop to re-order them.  
13. Click **Save Control Policy**. |
### Topology Type

<table>
<thead>
<tr>
<th>Description</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Centralized TLOC control policy (for matching TLOC routes)</td>
<td>1. In the Add Topology drop-down, select <strong>Custom Control (Route &amp; TLOC)</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. Enter a name for the control policy.</td>
</tr>
<tr>
<td></td>
<td>3. Enter a description for the policy.</td>
</tr>
<tr>
<td></td>
<td>4. In the left pane, click <strong>Add Sequence Type</strong>. The Add Control Policy popup displays.</td>
</tr>
<tr>
<td></td>
<td>5. Select TLOC. A policy component containing the text string TLOC is added in the left pane.</td>
</tr>
<tr>
<td></td>
<td>6. Double-click the TLOC text string, and enter a name for the policy component.</td>
</tr>
<tr>
<td></td>
<td>7. In the right pane, click <strong>Add Sequence Rule</strong>. The Match/Actions box opens, and Match is selected by default.</td>
</tr>
<tr>
<td></td>
<td>8. From the boxes under the Match box, select the desired policy match type. Then select or enter the value for that match condition. Configure additional match conditions for the sequence rule, as desired. For an explanation of the match conditions, see the OMP TLOC Match Attributes section in the Configuring Centralized Control Policy topic for your software release.</td>
</tr>
<tr>
<td></td>
<td>9. Click <strong>Actions</strong>. The Reject radio button is selected by default. To configure actions to perform on accepted packets, click the <strong>Accept</strong> radio button. Then select the action or enter a value for the action. For an explanation of the actions, see the Action Parameters section in the Configuring Centralized Control Policy topic for your software release.</td>
</tr>
<tr>
<td></td>
<td>10. Click <strong>Save Match and Actions</strong>.</td>
</tr>
<tr>
<td></td>
<td>11. Click <strong>Add Sequence Rules</strong> to configure more sequence rules, as desired. Drag and drop to re-order them.</td>
</tr>
<tr>
<td></td>
<td>12. Click <strong>Add Sequence Type</strong> to configure more sequences, as desired. Drag and drop to re-order them.</td>
</tr>
<tr>
<td></td>
<td>13. Click <strong>Save Control Policy</strong>.</td>
</tr>
</tbody>
</table>

1. **To use an existing topology:**

   a. In the **Add Topology** drop-down, click **Import Existing Topology**. The Import Existing Topology popup appears.

   b. Select the type of topology.

   c. In the **Policy** drop-down, choose the name of the topology.

   d. Click **Import**.

2. Click **Next** to move to **Configure Traffic Rules** in the wizard.
3. Click **Next** to move to **Apply Policies to Sites and VPNs** in the wizard.

**Step 4: Apply Policies to Sites and VPNs**

In **Apply Policies to Sites and VPNs** screen, apply a policy to sites and VPNs:

1. In the **Policy Name** field, enter a name for the policy. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores (_). It cannot contain spaces or any other characters.

2. In the **Policy Description** field, enter a description of the policy. It can contain up to 2048 characters. This field is mandatory, and it can contain any characters and spaces.

3. From the **Topology** bar, choose the type of policy block. The table then lists policies that you have created for that type of policy block.

4. Associate the policy with VPNs and sites. The choice of VPNs and sites depends on the type of policy block:
   - **a.** For a Topology policy block, click **Add New Site List** and **VPN List** or **Add New Site**. Some topology blocks might have no **Add** buttons. Choose one or more site lists, and choose one or more VPN lists. Click **Add**.
   - **b.** For an Application-Aware Routing policy block, click **Add New Site List** and **VPN list**. Choose one or more site lists, and choose one or more VPN lists. Click **Add**.
   - **c.** For a Traffic Data policy block, click **Add New Site List** and **VPN List**. Choose the direction for applying the policy (From Tunnel, From Service, or All), choose one or more site lists, and choose one or more VPN lists. Click **Add**.
   - **d.** For a cflowd policy block, click **Add New Site List**. Choose one or more site lists, Click **Add**.

5. Click **Preview** to view the configured policy. The policy appears in CLI format.

6. Click **Save** Policy. The **Configuration > Policies** screen appears, and the policies table includes the newly created policy.

**Step 5: Activate a Centralized Policy**

Activating a centralized policy sends that policy to all connected Cisco vSmart controllers. To activate a centralized policy:

1. In the Cisco vManage NMS, select the **Configure > Policies** screen. When you first open this screen, the **Centralized Policy** tab is selected by default.

2. Choose a policy.

3. Click the **More Actions** icon to the right of the row, and click **Activate**. The Activate Policy popup appears. It lists the IP addresses of the reachable Cisco vSmart Controllers to which the policy must be applied.

4. Click **Activate**.
Configure Centralized Policy Using CLI

To configure a centralized control policy using the CLI:

1. Create a list of overlay network sites to which the centralized control policy is to be applied (in the `apply-policy` command):
   
   ```
   vSmart(config)# policy
   vSmart(config-policy)# lists site-list list-name
   vSmart(config-lists-list-name)# site-id site-id
   ```

   The list can contain as many site IDs as necessary. Include one `site-id` command for each site ID. For contiguous site IDs, you can specify a range of numbers separated with a dash (–). Create additional site lists, as needed.

2. Create lists of IP prefixes, TLOCs, and VPNs as needed:
   
   ```
   vSmart(config)# policy lists
   vSmart(config-lists)# prefix-list list-name
   vSmart(config-lists-list-name)# ip-prefix prefix/length
   vSmart(config)# policy lists
   vSmart(config-lists)# tloc-list list-name
   vSmart(config-lists-list-name)# tloc address
   color
   ```

   ```
   vSmart(config)# policy lists
   vSmart(config-lists)# vpn-list list-name
   vSmart(config-lists-list-name)# vpn vpn-id
   ```

3. Create a control policy instance:
   
   ```
   vSmart(config)# policy control-policy policy-name
   vSmart(config-control-policy-policy-name)#
   ```

4. Create a series of match–action pair sequences:
   
   ```
   vSmart(config-control-policy-policy-name)# sequence number
   vSmart(config-sequence-number)#
   ```

   The match–action pairs are evaluated in order, by sequence number, starting with the lowest numbered pair and ending when the route matches the conditions in one of the pairs. Or if no match occurs, the default action is taken (either rejecting the route or accepting it as is).

5. Define match parameters for routes and for TLOCs:
   
   ```
   vSmart(config-sequence-number)# match route route-parameter
   vSmart(config-sequence-number)# match tloc tloc-parameter
   ```

6. Define actions to take when a match occurs:
   
   ```
   vSmart(config-sequence-number)# action reject
   vSmart(config-sequence-number)# action accept export-to (vpn vpn-id | vpn-list list-name)
   vSmart(config-sequence-number)# action accept set omp-tag number
   vSmart(config-sequence-number)# action accept set preference value
   ```
5. Create additional numbered sequences of match–action pairs within the control policy, as needed.

6. If a route does not match any of the conditions in one of the sequences, it is rejected by default. If you want nonmatching routes to be accepted, configure the default action for the policy:

```markdown
vSmart(config-policy-name)# default-action accept
```

7. Apply the policy to one or more sites in the Cisco SD-WAN overlay network:

```markdown
vSmart(config)# apply-policy site-list
list-name
control-policy
policy-name (in | out)
```

8. If the action you are configuring is a service, configure the required services on the Cisco devices so that the Cisco vSmart Controller knows how to reach the services:

```markdown
vEdge(config)# vpn vpn-id
service service-name
address ip-address
```

Specify the VPN is which the service is located and one to four IP addresses to reach the service device or devices. If multiple devices provide the same service, the Cisco device load-balances the traffic among them. Note that the Cisco device keeps track of the services, advertising them to the Cisco vSmart Controller only if the address (or one of the addresses) can be resolved locally, that is, at the Cisco device's local site, and not learned through OMP. If a previously advertised service becomes unavailable, the Cisco device withdraws the service advertisement.

### Structural Components for Centralized Control Policy

Following are the structural components required to configure centralized control policy. Each one is explained in more detail in the sections below.

```markdown
policy lists color-list list-name color color prefix-list list-name ip-prefix prefix site-list list-name site-id site-id tloc-list list-name tloc address color color
encap encapsulation [preference value] vpn-list list-name vpn vpn-id
control-policy
policy-name
sequence
number
match
match-parameters
action reject accept export-to vpn accept set parameter
default-action (accept | reject) apply-policy site-list list-name control-policy policy-name
(in | out)
```
### Lists

Centralized control policy uses the following types of lists to group related items. In the CLI, you configure lists under the `policy lists` command hierarchy on Cisco vSmart Controllers.

<table>
<thead>
<tr>
<th>List Type</th>
<th>Description</th>
<th>vManage Configuration/CLI Configuration Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Colors</td>
<td>List of one or more TLOC colors. <code>color</code> can be <code>3g</code>, <code>biz-internet</code>, <code>blue</code>, <code>bronze</code>, <code>custom1</code> through <code>custom3</code>, <code>default</code>, <code>gold</code>, <code>green</code>, <code>lte</code>, <code>metro-ethernet</code>, <code>mpls</code>, <code>private1</code> through <code>private6</code>, <code>red</code>, and <code>silver</code>. To configure multiple colors in a single list, include multiple <code>color</code> options, specifying one color in each option.</td>
<td>Configuration &gt; Policies &gt; Centralized Policy &gt; Add Policy &gt; Create Groups of Interest &gt; Color Configuration &gt; Policies &gt; Custom Options &gt; Centralized Policy &gt; Lists &gt; Color color-list list-name color</td>
</tr>
<tr>
<td>Prefixes</td>
<td>List of one or more IP prefixes. Specify the IP prefixes as follows: • <code>prefix/length</code>—Exactly match a single prefix–length pair. • <code>0.0.0.0/0</code>—Match any prefix–length pair. • <code>0.0.0.0/0 le length</code>—Match any IP prefix whose length is less than or equal to <code>length</code>. For example, <code>ip-prefix 0.0.0.0/0 le 16</code> matches all IP prefixes with lengths from /1 through /16. • <code>0.0.0.0/0 ge length</code>—Match any IP prefix whose length is greater than or equal to <code>length</code>. For example, <code>ip-prefix 0.0.0.0/0 ge 25</code> matches all IP prefixes with lengths from /25 through /32. • <code>0.0.0.0/0 ge length1 le length2</code>, or <code>0.0.0.0/0 ge length1 le length2 ge length1</code>—Match any IP prefix whose length is greater than or equal to <code>length1</code> and less than or equal to <code>length2</code>. For example, <code>ip-prefix 0.0.0.0/0 ge 20 le 24</code> matches all /20, /21, /22, /23, and /24 prefixes. Also, <code>ip-prefix 0.0.0.0/0 ge 20 le 24 ge 20</code> matches the same prefixes. If <code>length1</code> and <code>length2</code> are the same, a single IP prefix length is matched. For example, <code>ip-prefix 0.0.0.0/0 ge 24 le 24</code> matches only /24 prefixes. To configure multiple prefixes in a single list, include multiple <code>ip-prefix</code> options, specifying one prefix in each option.</td>
<td>Configuration &gt; Policies &gt; Centralized Policy &gt; Add Policy &gt; Create Groups of Interest &gt; Prefix Configuration &gt; Policies &gt; Custom Options &gt; Centralized Policy &gt; Lists &gt; Prefix prefix-list list-name ip-prefix prefix/length</td>
</tr>
<tr>
<td>Sites</td>
<td>List of one or more site identifiers in the overlay network. You can specify a single site identifier (such as <code>site-id 1</code>) or a range of site identifiers (such as <code>site-id 1-10</code>). To configure multiple sites in a single list, include multiple <code>site-id</code> options, specifying one site number in each option.</td>
<td>Configuration &gt; Policies &gt; Centralized Policy &gt; Add Policy &gt; Create Groups of Interest &gt; Site Configuration &gt; Policies &gt; Custom Options &gt; Centralized Policy &gt; Lists &gt; Site site-list list-name site-id site-id</td>
</tr>
</tbody>
</table>
### Structural Components for Centralized Control Policy

<table>
<thead>
<tr>
<th>List Type</th>
<th>Description</th>
<th>vManage Configuration/ CLI Configuration Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLOCs</td>
<td>List of one or more TLOCs in the overlay network. For each TLOC, specify its address, color, and encapsulation. address is the system IP address, color can be one of 3g, biz-internet, blue, bronze, custom1, custom2, custom3, default, gold, green, lte, metro-ethernet, mpls, privatel through private6, public-internet, red, and silver. encapsulation can be gre or ipsec. Optionally, set a preference value (from 0 to 2^{32} – 1) to associate with the TLOC address. When you apply a TLOC list in an action accept condition, when multiple TLOCs are available and satisfy the match conditions, the TLOC with the lowest preference value is used. If two or more of TLOCs have the lowest preference value, traffic is sent among them in an ECMP fashion.</td>
<td>Configuration &gt; Policies &gt; Centralized Policy &gt; Add Policy &gt; Create Groups of Interest &gt; TLOC tloc-list list-name tloc ip-address color [encap (gre</td>
</tr>
<tr>
<td>VPNS</td>
<td>List of one or more VPNS in the overlay network. For data policy, you can configure any VPNS except for VPN 0 and VPN 512. To configure multiple VPNS in a single list, include multiple vpn options, specifying one VPN number in each option. You can specify a single VPN identifier (such as vpn 1) or a range of VPN identifiers (such as vpn 1-10).</td>
<td>Configuration &gt; Policies &gt; Centralized Policy &gt; Add Policy &gt; Create Groups of Interest &gt; VPNS vpn-list list-namevpn vpn-id</td>
</tr>
</tbody>
</table>

### Sequences

A centralized control policy contains sequences of match–action pairs. The sequences are numbered to set the order in which a route or TLOC is analyzed by the match–action pairs in the policy.

In the Cisco vManage NMS, you configure sequences from:

- Configuration > Policies > Centralized Policy > Add Policy > Configure Traffic Rules > (Application-Aware Routing | Traffic Data | Cflowd) > Sequence Type
- Configuration > Policies > Custom Options > Centralized Policy > Traffic Policy > (Application-Aware Routing | Traffic Data | Cflowd) > Sequence Type

In the CLI, you configure sequences with the `policy control-policy sequence` command.

Each sequence in a centralized control policy can contain one match condition (either for a route or for a TLOC) and one action condition.

### Match Parameters

Centralized control policy can match OMP route or TLOC route attributes.

In the Cisco vManage NMS, you configure match parameters from:

- Configuration > Policies > Centralized Policy > Add Policy > Configure Topology and VPN Membership > Add Topology > Custom Control (Route & TLOC) > Sequence Type > (Route | TLOC) > Sequence Rule > Match

---

**Policies Configuration Guide for vEdge Routers, Cisco SD-WAN Releases 19.1, 19.2, and 19.3**
In the CLI, you configure the OMP route attributes to match with the `policy control-policy sequence match route` command, and you configure the TLOC attributes to match with the `policy control-policy sequence match tloc` command.

Each sequence in a policy can contain one `match` section—either `match route` or `match tloc`.

**OMP Route Match Attributes**

For OMP routes (vRoutes), you can match these attributes:

<table>
<thead>
<tr>
<th>Description</th>
<th>vManage Configuration/ CLI Configuration Command</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individual color.</td>
<td>Not available in the Cisco vManage NMS.</td>
<td>3g, biz-internet, blue, bronze, custom1 through custom3, default, gold, green, lte, metro-ethernet, mpls, private1 through private6, public-internet, red, and silver</td>
</tr>
<tr>
<td>One or more colors.</td>
<td>Match Color List</td>
<td>Name of a color or a policy lists color-list list.</td>
</tr>
<tr>
<td>Tag value associated with the route or prefix in</td>
<td>Match OMP Tag</td>
<td>0 through 4294967295</td>
</tr>
<tr>
<td>the routing database on the Cisco device.</td>
<td><code>omp-tag number</code></td>
<td></td>
</tr>
<tr>
<td>Protocol from which the route was learned.</td>
<td>Match Origin</td>
<td>bgp-external, bgp-internal, connected, ospf-external1, ospf-external2, ospf-inter-area, ospf-intra-area, static</td>
</tr>
<tr>
<td>IP address from which the route was learned.</td>
<td>Match Originator</td>
<td>IP address</td>
</tr>
<tr>
<td>How preferred a prefix is. This is the preference</td>
<td>Match Preference</td>
<td>0 through 255</td>
</tr>
<tr>
<td>value that the route or prefix has in the local</td>
<td><code>preference number</code></td>
<td></td>
</tr>
<tr>
<td>site, that is, in the routing database on the</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco device. A higher preference value is more</td>
<td></td>
<td></td>
</tr>
<tr>
<td>preferred.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>One or more prefixes.</td>
<td>Match Prefix List</td>
<td>Name of a prefix list or a policy lists prefix-list list.</td>
</tr>
<tr>
<td>Individual site identifier.</td>
<td>Not available in Cisco vManage.</td>
<td>0 through 4294967295</td>
</tr>
<tr>
<td>One or more overlay network site identifiers.</td>
<td>Match Site</td>
<td>Name of a site or a policy lists site-list list.</td>
</tr>
<tr>
<td>Description</td>
<td>vManage Configuration/ CLI Configuration Command</td>
<td>Value or Range</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>-------------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Individual TLOC address.</td>
<td>Match TLOC tloc ip-address</td>
<td>IP address</td>
</tr>
<tr>
<td>One or more TLOC addresses.</td>
<td>Match TLOC tloc-list list-name</td>
<td>Name of a TLOC or a policy lists tloc-list list.</td>
</tr>
<tr>
<td>Individual VPN identifier.</td>
<td>Match VPN vpn vpn-id</td>
<td>0 through 65535</td>
</tr>
<tr>
<td>One or more VPN identifiers.</td>
<td>Match VPN vpn-list list-name</td>
<td>Name of a VPN or a policy lists vpn-list list.</td>
</tr>
</tbody>
</table>

**TLOC Route Match Attributes**

For TLOC routes, you can match these attributes:

<table>
<thead>
<tr>
<th>Description</th>
<th>vManage Configuration/ CLI Configuration Command</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Carrier for the control traffic.</td>
<td>Match Carrier carrier carrier-name</td>
<td>default, carrier1 through carrier8</td>
</tr>
<tr>
<td>Individual color.</td>
<td>Not available in the Cisco vManage NMS.</td>
<td>3g, biz-internet, blue, bronze, custom1 through custom3, default, gold, green, lte, metro-ethernet, mpls, private1 through private6, public-internet, red, and silver</td>
</tr>
<tr>
<td>One or more colors.</td>
<td>Match Color List color-list list-name</td>
<td>See the colors above.</td>
</tr>
<tr>
<td>Domain identifier associated with a TLOC.</td>
<td>Match Domain ID domain-id domain-id</td>
<td>0 through 4294967295</td>
</tr>
<tr>
<td>Tag value associated with the TLOC route in the route table on the Cisco device.</td>
<td>Match OMP Tag omp-tag number</td>
<td>0 through 4294967295</td>
</tr>
<tr>
<td>IP address from which the route was learned.</td>
<td>Match Originator originator ip-address</td>
<td>IP address</td>
</tr>
<tr>
<td>Description</td>
<td>vManage Configuration/ CLI Configuration Command</td>
<td>Value or Range</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>How preferred a TLOC route is. This is the preference value that the TLOC route has in the local site, that is, in the route table on the Cisco device. A higher preference value is more preferred.</td>
<td>Match Preference preference number</td>
<td>0 through 255</td>
</tr>
<tr>
<td>Individual site identifier.</td>
<td>Match Site site-id</td>
<td>0 through 4294967295</td>
</tr>
<tr>
<td>One or more overlay network site identifiers.</td>
<td>Match Site site-list list-name</td>
<td>Name of a policy lists site-list list.</td>
</tr>
<tr>
<td>Individual TLOC address.</td>
<td>Match TLOC tloc address</td>
<td>IP address</td>
</tr>
<tr>
<td>One or more TLOC addresses.</td>
<td>Match TLOC tloc-list list-name</td>
<td>Name of a policy lists tloc-list list.</td>
</tr>
</tbody>
</table>

**Action Parameters**

For each match condition, you configure a corresponding action to take if the route or TLOC matches.

In the Cisco vManage NMS, you configure match parameters from:

- **Configuration > Policies > Centralized Policy > Add Policy > Configure Topology and VPN Membership > Add Topology > Custom Control (Route & TLOC) > Sequence Type > (Route | TLOC) > Sequence Rule > Action**

- **Configuration > Policies > Custom Options > Centralized Policy > Topology > Add Topology > Custom Control (Route & TLOC) > Sequence Type > (Route | TLOC) > Sequence Rule > Action**

In the CLI, you configure actions with the `policy control-policy action` command.

Each sequence in a centralized control policy can contain one action condition.

In the action, you first specify whether to accept or reject a matching route or TLOC:

<table>
<thead>
<tr>
<th>Description</th>
<th>vManage Configuration/ CLI Configuration Command</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept the route. An accepted route is eligible to be modified by the additional parameters configured in the action portion of the policy configuration.</td>
<td>Click Accept. accept</td>
<td>—</td>
</tr>
<tr>
<td>Discard the packet.</td>
<td>Click Reject. reject</td>
<td>—</td>
</tr>
</tbody>
</table>

Then, for a route or TLOC that is accepted, you can configure the following actions:
<table>
<thead>
<tr>
<th>Description</th>
<th>vManage Configuration/ CLI Configuration Command</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export the route the the specified VPN or list of VPNs (for a <strong>match route</strong> match condition only).</td>
<td>Click <strong>Accept</strong>, then action <strong>Export To.</strong> export-to (vpn vpn-id</td>
<td>0 through 65535 or list name.</td>
</tr>
<tr>
<td>Change the tag string in the route, prefix, or TLOC.</td>
<td>Click <strong>Accept</strong>, then action <strong>OMP Tag.</strong> set omp-tag number</td>
<td>0 through 4294967295</td>
</tr>
<tr>
<td>Change the preference value in the route, prefix, or TLOC to the specified value. A higher preference value is more preferred.</td>
<td>Click <strong>Accept</strong>, then action <strong>Preference.</strong> set preference number</td>
<td>0 through 255</td>
</tr>
<tr>
<td>Specify a service to redirect traffic to before delivering the traffic to its destination.</td>
<td>Click <strong>Accept</strong>, then action <strong>Service.</strong> set service service-name (tloc ip-address</td>
<td>Standard services: FW, IDS, IDP Custom services: netsvc1, netsvc2, netsvc3, netsvc4</td>
</tr>
<tr>
<td>The TLOC address or list of TLOCs identifies the TLOCs to which the traffic should be redirected to reach the service. In the case of multiple TLOCs, the traffic is load-balanced among them.</td>
<td>tloc-list list-name) [vpn vpn-id]</td>
<td>TLOC list configured with a <strong>policy lists tloc-list</strong> command.</td>
</tr>
<tr>
<td>The VPN identifier is where the service is located.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure the services themselves on the Cisco devices that are colocated with the service devices, using the <strong>vpn service</strong> configuration command.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Change the TLOC address, color, and encapsulation to the specified address and color.</td>
<td>Click <strong>Accept</strong>, then action <strong>TLOC.</strong> set tloc ip-address color color [encap encapsulation]</td>
<td>IP address, TLOC color, and encapsulation, Color can be one of 3g, biz-internet, blue, bronze, custom1 through custom3, default, gold, green, lte, metro-ethernet, mpls, private1 through private6, public-internet, red, and silver. Encapsulation can be either gre or ipsec.</td>
</tr>
<tr>
<td>Description</td>
<td>vManage Configuration/ CLI Configuration Command</td>
<td>Value or Range</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------</td>
<td>----------------</td>
</tr>
</tbody>
</table>
| Direct matching routes or TLOCs using the mechanism specified by action, and enable end-to-end tracking of whether the ultimate destination is reachable. Setting a TLOC action is useful when traffic is first directed, via policy, to an intermediate destination, which then forwards the traffic to its ultimate destination. For example, for traffic from Device-A destined for Device-D, a policy might direct traffic from Device-A first to Device-B (the intermediate destination), and Device-B then sends it to the final destination, Device-D. Setting the TLOC action option enables the Cisco vSmart Controller to perform end-to-end tracking of the path to the ultimate destination router. In our example, matching traffic goes from Device-A to Device-B and then, in a single hop, goes to Device-D. If the tunnel between Device-B and Device-D goes down, the Cisco vSmart Controller relays this information to Device-A, and Device-A removes its route to Device-D from its local route table. End-to-end tracking works here only because traffic goes from Device-B to Device-D in a single hop, via a single tunnel. If the traffic from Device-A went first to Device-B, then to Device-C, and finally to Device-D, the Cisco vSmart Controller is unable to perform end-to-end tracking and is thus unable to keep Device-A informed about whether full path between it and Device-D is up. | Click **Accept**, then action **TLOC Action.**
set tloc-action **action** | **ecmp**—Equally direct matching control traffic between the intermediate destination and the ultimate destination. In our example, traffic would be sent to Device-B (which would then send it to Device-D) and directly to Device-D. With this action, if the intermediate destination is down, all traffic reaches the ultimate destination. | **primary**—First direct matching traffic to the intermediate destination. If that router is not reachable, then direct it to the final destination. In our example, traffic would first be sent to Device-B. If this router is down, it is sent directly to Device-D. With this action, if the intermediate destination is down, all traffic reaches the final destination. | **backup**—First direct matching traffic to the final destination. If that router is not reachable, then direct it to the intermediate destination. In our example, traffic would first be sent directly to Device-D. If the Device-A is not able to reach Device-D, traffic is sent to Device-B, which might have an operational path to reach Device-D. With this action, if the source is unable to reach the final destination directly, it is possible for all traffic to reach the final destination via the intermediate destination. | **strict**—Direct matching traffic only to the intermediate destination. In our example, traffic is sent only to Device-B, regardless of whether it is reachable. With this action, if the intermediate destination is down, no traffic reaches the final destination. If you do not configure a set tloc-action action in a centralized control policy, strict is the default behavior. |
| Change the TLOC address and color to those in the specified TLOC list. | Click **Accept**, then action **TLOC.**
set tloc-list **list-name** | **Name of a policy lists tloc-list list.** |
Default Action

If a route or TLOC being evaluated does not match any of the match conditions in a centralized control policy, a default action is applied to it. By default, the route or TLOC is rejected.

In the Cisco vManage NMS, you modify the default action from Configuration > Policies > Centralized Policy > Add Policy > Configure Topology and VPN Membership > Add Topology > Custom Control (Route and TLOC) > Sequence Type > (Route | TLOC) > Sequence Rule > Default Action.

In the CLI, you modify the default action with the control policy default-action accept command.

Apply Centralized Control Policy

For a centralized control policy to take effect, you apply it to a list of sites in the overlay network.

To apply a centralized policy in the Cisco vManage NMS:

1. In the Cisco vManage NMS, select the Configure > Policies screen.
2. Select a policy from the policy table.
3. Click the More Actions icon to the right of the row, and click Activate. The Activate Policy popup opens. It lists the IP addresses of the reachable Cisco vSmart Controllers to which the policy is to be applied.
4. Click Activate.

To apply a centralized policy in the CLI:

```sh
vSmart(config)# apply-policy
site-list list-name control-policy policy-name (in | out)
```

You apply centralized control policy directionally:

- Inbound direction (in)—The policy analyzes routes and TLOCs being received from the sites in the site list before placing the routes and TLOCs into the route table on the Cisco vSmart Controller, so the specified policy actions affect the OMP routes stored in the route table.

- Outbound direction (out)—The policy analyzes routes and TLOCs in the Cisco vSmart Controller's route table after they are exported from the route table.

For all control-policy policies that you apply with apply-policy commands, the site IDs across all the site lists must be unique. That is, the site lists must not contain overlapping site IDs. An example of overlapping site IDs are those in the two site lists site-list 1 site-id 1-100 and site-list 2 site-id 70-130. Here, sites 70 through 100 are in both lists. If you were to apply these two site lists to two different control-policy policies, the attempt to commit the configuration on the Cisco vSmart Controller would fail.

The same type of restriction also applies to the following types of policies:

- Application-aware routing policy (app-route-policy)
- Centralized data policy (data-policy)
- Centralized data policy used for cflowd flow monitoring (data-policy hat includes a cflowd action and apply-policy that includes a cflowd-template command)
You can, however, have overlapping site IDs for site lists that you apply for different types of policy. For example, the sites lists for control-policy and data-policy policies can have overlapping site IDs. So for the two example site lists above, site-list 1 site-id 1-100 and site-list 2 site-id 70-130, you could apply one to a control policy and the other to a data policy.

Centralized Control Policy Configuration Examples

This topic provides some straightforward examples of configuring centralized control policy to help you understand the configuration procedure and get an idea of how to use policy to influence traffic flow across the Cisco SD-WAN overlay network domain.

Traffic Engineering

This example of traffic engineering forces all traffic to come to a Cisco device using a device hub instead of directly.

One common way to design a domain in a Cisco SD-WAN overlay network is to route all traffic destined for branches through a hub router, which is typically located in a data center, rather than sending the traffic directly from one Cisco device to another. You can think of this as a hub-and-spoke design, where one Cisco device is acting as a hub and the Cisco devices are the spokes. With such a design, traffic between local branches travels over the IPsec connections that are established between the spoke routers and the hub routers when the Cisco devices are booted up. Using established connections means that the Cisco devices do not need to expend time and CPU cycles to establish IPsec connections with each other. If you were to imagine that this were a large network with many Cisco devices, having a full mesh of connections between each pair of routers would require a large amount of CPU from the routers. Another attribute of this design is that, from an administrative point of view, it can be simpler to institute coordinated traffic flow policies on the hub routers, both because there are fewer of them in the overlay network and because they are located in a centralized data center.

One way to direct all Cisco device spoke router traffic to a Cisco hub router is to create a policy that changes the TLOC associated with the routes in the local network. Let’s consider the topology in the figure here:
This topology has two Cisco devices in different branches:

- The Device West in site ID 1. The TLOC for this device is defined by its IP address (192.0.2.1), a color (gold), and an encapsulation (here, IPsec). We write the full TLOC address as {192.0.2.1, gold, ipsec}. The color is simply a way to identify a flow of traffic and to separate it from other flows.
- The Device East in site ID 2 has a TLOC address of {203.0.113.1, gold, ipsec}.

The devices West and East learn each other’s TLOC addresses from the OMP routes distributed to them by the Cisco vSmart Controller. In this example, the Device East advertises the prefix 209.165.201.0/27 as being reachable at TLOC {203.0.113.1, gold, }. In the absence of any policy, the Device West could route traffic destined for 209.165.201.0/27 to TLOC {203.0.113.1, gold, ipsec}, which means that the Device West would be sending traffic directly to the Device East.

However, our design requires that all traffic from West to East be routed through the hub router, whose TLOC address is {209.165.200.225, gold, ipsec}, before going to the Device East. To effect this traffic flow, you define a policy that changes the route's TLOC. So, for the prefix 1209.165.201.0/27, you create a policy that changes the TLOC associated with the prefix 209.165.201.0/27 from {203.0.113.1, gold, ipsec}, which is the TLOC address of the Device East, to {209.165.200.225, gold, ipsec}, which is the TLOC address of the hub router. The result is that the OMP route for the prefix 209.165.201.0/27 that the Cisco vSmart Controller advertises to the Device West that contains the TLOC address of the hub router instead of the TLOC address of the Device East. From a traffic flow point of view, the Device West then sends all traffic destined for 209.165.201.0/27 to the hub router.

The Cisco device also learns the TLOC addresses of the West and East devices from the OMP routes advertised by the Cisco vSmart Controller. Because we want Cisco devices to use these two TLOC addresses, no policy is required to control how the hub directs traffic to the Cisco devices.

Here is a policy configuration on the Cisco vSmart Controller that directs the Device West (and any other Cisco devices in the network domain) to send traffic destined to prefix 209.165.201.0/27 to TLOC 209.165.200.225, gold, which is the Cisco device:

```
policy
  lists
    prefix-list east-prefixes
    ip-prefix 209.165.201.0/27
    site-list west-sites
    site-id 1
  control-policy change-tloc
  sequence 10
    match route
      prefix-list east-prefixes
      site-id 2
    action accept
      set tloc 209.165.200.225 color gold encap ipsec
  apply-policy
    site west-sites control-policy change-tloc out
```

A rough English translation of this policy is:

Create a list named “east-prefixes” that contains the IP prefix “209.165.201.0/27”
Create a list named “west-sites” that contains the site-id “1”
Define a control policy named “change-tloc”
Create a policy sequence element that:
  Matches a prefix from list “east-prefixes”, that is, matches “209.165.201.0/27”
  AND matches a route from site-id “2”
If a match occurs:
  Accept the route
  AND change the route’s TLOC to “209.165.200.225” with a color of "gold" and an encapsulation of "ipsec"
Apply the control policy "change-tloc" to OMP routes sent by the vSmart controller to "west-sites", that is, to site ID 1

This control policy is configured on the Cisco vSmart Controller as an outbound policy, as indicated by the out option in the apply-policy site command. This option means the Cisco vSmart Controller applies the TLOC change to the OMP route after it distributes the route from its route table. The OMP route for prefix 209.165.201.0/27 that the Cisco vSmart Controller distributes to the Device West associates 209.165.201.0/27 with TLOC 209.165.200.225, gold. This is the OMP route that the Device West installs it in its route table. The end results are that when the Device West sends traffic to 209.165.201.0/27, the traffic is directed to the hub; and the Device West does not establish a DTLS tunnel directly with the Device East.

If the West side of the network had many sites instead of just one and each site had its own Cisco device, it would be straightforward to apply this same policy to all the sites. To do this, you simply add the site IDs of all the sites in the site-list west-sites list. This is the only change you need to make in the policy to have all the West-side sites send traffic bound for the prefix 209.165.201.0/27 through the Cisco device. For example:

```plaintext
policy lists
   prefix-list east-prefixes
     ip-prefix 209.165.201.0/27
   site-list west-sites
     site-id 1
     site-id 11
     site-id 12
     site-id 13
   control-policy change-tloc
     sequence 10
     match route
       prefix-list east-prefixes
       site-id 2
     action accept
       set tloc 209.165.200.225 color gold encap ipsec
   apply-policy
     site west-sites control-policy change-tloc out
```

Creating Arbitrary Topologies

To provide redundancy in the hub-and-spoke-style topology discussed in the previous example, you can add a second Cisco hub to create a dual-homed hub site. The following figure shows that site ID 10 now has two Cisco Device hubs. We still want all inter-branch traffic to be routed through a device hub. However, because we now have dual-homed hubs, we want to share the data traffic between the two hub routers.

- Device Hub West, with TLOC 209.165.200.225, gold. We want all data traffic from branches on the West side of the overlay network to pass through and be processed by this device.
- Device Hub East, with TLOC 198.51.100.1, gold. Similarly, we all East-side data traffic to pass through the Device Hub East.
Here is a policy configuration on the Cisco vSmart Controller that would send West-side data traffic through the Cisco hub, and West and East-side traffic through the Device Hub East:

```
policy
  lists
    site-list west-sites
    site-id 1
    site-list east-sites
    site-id 2
  tloc-list west-hub-tlocs
    tloc-id 209.165.200.225 gold
    tloc-id 198.51.100.1 gold
control-policy prefer-west-hub
  sequence 10
  match tloc
    tloc-list west-hub-tlocs
  action accept
    set preference 50
control-policy prefer-east-hub
  sequence 10
  match tloc
    tloc-list east-hub-tlocs
  action accept
    set preference 50
apply-policy
  site west-sites control-policy prefer-west-hub out
  site east-sites control-policy prefer-east-hub out
```

Here is an explanation of this policy configuration:

Create the site lists that are required for the **apply-policy** configuration command:

- **site-list west-sites** lists all the site IDs for all the devices in the West portion of the overlay network.
- **site-list east-sites** lists the site IDs for the devices in the East portion of the network.

Create the TLOC lists that are required for the match condition in the control policy:
• **west-hub-tlocs** lists the TLOC for the Device West Hub, which we want to service traffic from the West-side device.

• **east-hub-tlocs** lists the TLOC for the Device East Hub, to service traffic from the East devices.

Define two control policies:

• **prefer-west-hub** affects OMP routes destined to TLOC 209.165.200.225, gold, which is the TLOC address of the Device West hub router. This policy modifies the preference value in the OMP route to a value of 50, which is large enough that it is likely that no other OMP routes will have a larger preference. So setting a high preference value directs traffic destined for site 100 to the Device West hub router.

• Similarly, **prefer-east-hub** sets the preference to 50 for OMP routes destined TLOC 198.51.100.1, gold, which is the TLOC address of the Device East hub router, thus directing traffic destined for site 100 site to the Device East hub router.

Apply the control policies:

• The first line in the `apply-policy` configuration has the Cisco vSmart Controller apply the **prefer-west-hub** control policy to the sites listed in the `west-sites` list, which here is only site ID 1, so that the preference in their OMP routes destined to TLOC 209.165.200.225 is changed to 50 and traffic sent from the Device West to the hub site goes through the Device West hub router.

• The Cisco vSmart Controller applies the **prefer-east-hub** control policy to the OMP routes that it advertises to the Cisco devices in the `east-sites` list, which changes the preference to 50 for OMP routes destined to TLOC 198.51.100.1, so that traffic from the Device East goes to the Device East hub router.

---

### Localized Control Policy

Control policy operates on the control plane traffic in the Cisco SD-WAN overlay network, influencing the determination of routing paths through the overlay network. Localized control policy is policy that is configured on a Cisco device (hence, it is local) and affects BGP and OSPF routing decisions on the site-local network that the Cisco device is part of.

In addition to participating in the overlay network, a Cisco device participates in the network at its local site, where it appears to the other network devices to be simply a regular router. As such, you can provision routing protocols, such as BGP and OSPF, on the Cisco device so that it can exchange route information with the local-site routers. To control and modify the routing behavior on the local network, you configure a type of control policy called route policy on the Cisco devices. Route policy applies only to routing performed at the local branch, and it affects only the route table entries in the local Cisco device's route table.

Localized control policy, which you configure on Cisco devices, lets you affect routing policy on the network at the local site where the Cisco device is located. This type of control policy is called route policy.

### Configuration Components

A route policy consists of a series of numbered (ordered) sequences of match-action pair that are evaluated in order, from lowest sequence number to highest sequence number. When a packet matches one of the match conditions, the associated action is taken and policy evaluation on that packets stops. Keep this in mind as you design your policies to ensure that the desired actions are taken on the items subject to policy.

If a packet matches no parameters in any of the sequences in the policy configured, it is, by default, rejected and discarded.
Configure Localized Control Policy Using Cisco vManage

To configure localized policies, use the Cisco vManage policy configuration wizard. The wizard is a UI policy builder that consists of five screens to configure and modify the following localized policy components:

- Groups of interest, also called lists
- Forwarding classes to use for QoS
- Access control lists (ACLs)
- Route policies
- Policy settings

You configure some or all these components depending on the specific policy you are creating. To skip a component, click the Next button at the bottom of the screen. To return to a component, click the Back button at the bottom of the screen.

Step 1: Start the Policy Configuration Wizard

To start the policy configuration wizard:

1. In the Cisco vManage NMS, select the Configure > Policies screen.
2. Select the Localized Policy tab.
3. Click Add Policy.

The policy configuration wizard opens, and the Create Groups of Interest screen is displayed.

Step 2: Configure Groups of Interest

In Create Groups of Interest, create lists of groups to use in localized policy:
1. Create new lists, as described in the following table:

**Table 6:**

<table>
<thead>
<tr>
<th>List Type</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| AS Path     | 1. In the left bar, click **AS Path**.  
2. Click **New AS Path List**.  
3. Enter a name for the list.  
4. Enter the AS path, separating AS numbers with a comma.  
5. Click **Add**. |
| Community   | 1. In the left bar, click **Community**.  
2. Click **New Community List**.  
3. Enter a name for the list.  
4. Enter the BGP community in the format *aa:*nn or as the string **internet**, **local-as**, **no-advertise**, or **no-export**, separating multiple items with a comma. For *aa*, enter a 2-byte AS number, and for *nn*, enter a 2-byte network number.  
5. Click **Add**. |
<table>
<thead>
<tr>
<th>List Type</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| Extended Community| 1. In the left bar, click **Extended Community**.  
2. Click **New Extended Community List**.  
3. Enter a name for the list.  
4. Enter the BGP extended community as rt *(aa:nn | ip-address)*, for a route target community, or soo *(aa:nn | ip-address)*, for a route origin community, separating multiple items with a comma. For aa, enter a 2-byte AS number, and for nn enter a 2-byte network number.  
5. Click **Add**. |
| Mirror            | 1. In the left bar, click **TLOC**.  
2. Click **New TLOC List**. The TLOC List popup displays.  
3. Enter a name for the list.  
4. In the TLOC IP field, enter the system IP address for the TLOC.  
5. In the Color field, select the TLOC’s color.  
6. In the Encap field, select the encapsulation type.  
7. In the Preference field, optionally select a preference to associate with the TLOC.  
8. Click **Add TLOC** to add another TLOC to the list.  
9. Click **Save**. |
| Policer           | 1. In the left bar, click **VPN**.  
2. Click **New VPN List**.  
3. Enter a name for the list.  
4. In the Add VPN field, enter one or more VPN IDs separated by commas.  
5. Click **Add**. |
<table>
<thead>
<tr>
<th>List Type</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| Prefix    | 1. In the left bar, click **Prefix**.  
           | 2. Click **New Prefix List**.  
           | 3. Enter a name for the list.  
           | 4. Enter the IP prefix in one of the following formats:  
               • **prefix/length**—Exactly match a single prefix–length pair.  
               • **0.0.0.0/0**—Match any prefix–length pair.  
               • **0.0.0.0/0 le length**—Match any IP prefix whose length is less than or equal to `length`. For example, `ip-prefix 0.0.0.0/0 le 16` matches all IP prefixes with lengths from /1 through /16.  
               • **0.0.0.0/0 ge length**—Match any IP prefix whose length is greater than or equal to `length`. For example, `ip-prefix 0.0.0.0/0 ge 25` matches all IP prefixes with lengths from /25 through /32.  
               • **0.0.0.0/0 ge length1 le length2**, or **0.0.0.0/0 le length2 ge length1**—Match any IP prefix whose length is greater than or equal to `length1` and less than or equal to `length2`. For example, `ip-prefix 0.0.0.0/0 ge 20 le 24` matches all /20, /21, /22, /23, and /24 prefixes. Also, `ip-prefix 0.0.0.0/0 le 24 ge 20` matches the same prefixes. If `length1` and `length2` are the same, a single IP prefix length is matched. For example, `ip-prefix 0.0.0.0/0 ge 24 le 24` matches only /24 prefixes.  
           | 5. Click **Add**. |

1. Click **Next** to move to Configure Forwarding Classes/QoS in the wizard.  
2. Click **Next** to move to Configure Access Control Lists in the wizard.  
3. Click **Next** to move to Configure Route Policies in the wizard.  

**Step 3: Configure Route Policies**

In Configure Route Policies, configure the routing policies:  
1. In the **Add Route Policy** tab, select **Create New**.  
2. Enter a name and description for the route policy.  
3. In the left pane, click **Add Sequence Type**. A Route box is displayed in the left pane.  
4. Double-click the **Route** box, and type a name for the route policy.  
5. In the right pane, click **Add Sequence Rule** to create a single sequence in the policy. The Match tab is selected by default.  
6. Click a match condition.  
7. On the left, enter the values for the match condition.  
8. On the right enter the action or actions to take if the policy matches.
9. Repeat Steps 6 through 8 to add match–action pairs to the route policy.
10. To rearrange match–action pairs in the route policy, in the right pane drag them to the desired position.
11. To remove a match–action pair from the route policy, click the X in the upper right of the condition.
12. Click **Save Match and Actions** to save a sequence rule.
13. To rearrange sequence rules in an route policy, in the left pane drag the rules to the desired position.
14. To copy, delete, or rename an route policy sequence rule, in the left pane, click **More Options** next to the rule's name and select the desired option.
15. If no packets match any of the route policy sequence rules, the default action is to drop the packets. To change the default action:
   a. Click **Default Action** in the left pane.
   b. Click the Pencil icon.
   c. Change the default action to Accept.
   d. Click **Save Match and Actions**.
16. Click **Next** to move to Policy Overview in the wizard.
17. Click **Preview** to view the full policy in CLI format.
18. Click **Save Policy**.

**Step 4: Apply a Route Policy in a Device Template**

1. In the Cisco vManage NMS, select the **Configuration > Templates** screen.
2. If you are creating a new device template:
   a. In the Device tab, click **Create Template**.
   b. From the Create Template drop-down, select **From Feature Template**.
   c. From the Device Model drop-down, select one of the Cisco devices.
   d. In the Template Name field, enter a name for the device template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores (_). It cannot contain spaces or any other characters.
   e. In the Description field, enter a description for the device template. This field is mandatory, and it can contain any characters and spaces.
   f. Continue with Step 4.
3. If you are editing an existing device template:
   a. In the Device tab, click the **More Actions** icon to the right of the desired template, and click the pencil icon.
   b. Click the **Additional Templates** tab. The screen scrolls to the Additional Templates section.
   c. From the Policy drop-down, select the name of a policy that you have configured.
4. Click the **Additional Templates** tab located directly beneath the Description field. The screen scrolls to the Additional Templates section.

5. From the Policy drop-down, select the name of the policy you configured in the above procedure.

6. To apply a route policy to BGP:
   a. Scroll to the Service VPN section.
   b. In the Service VPN drop-down, type the service VPN number (a VPN number other than 0 or 512).
   c. From Additional VPN Templates, select BGP.
   d. From the BGP drop-down, click **Create Template** or **View Template**.
   e. Select the **Neighbor** tab, click the plus sign (+), and click **More**.
   f. In Address Family, change the scope to Device Specific. Then, Click On to enable Address Family, Click On to enable Route Policy In, and specify the name of a route policy to apply to prefixes received from the neighbor, or Click On to enable Route Policy Out, and specify the name of a route policy to apply to prefixes sent to the neighbor. This name is one that you configured with a **policy route-policy** command.
   g. Click **Save** to save the neighbor configuration, and then click **Save** to save the BGP configuration.

7. To apply a route policy to routes coming from all OSPF neighbors:
   a. Scroll to the Service VPN section.
   b. In the Service VPN drop-down, type the service VPN number (a VPN number other than 0 or 512).
   c. From Additional VPN Templates, select **OSPF**.
   d. Click **Create Template** or **View Template**.
   e. Select the **Advanced** tab.
   f. In Policy Name, specify the name of a route policy to apply to incoming routes. This name is one that you configured with a **policy route-policy** command.
   g. Click **Save**.

8. To apply a route policy before redistributing routes into OSPF:
   a. Scroll to the Service VPN section.
   b. In the Service VPN drop-down, type the service VPN number (a VPN number other than 0 or 512).
   c. From Additional VPN Templates, select **OSPF**.
   d. Click **Create Template** or **View Template**.
   e. Select the **Redistribute** tab, click the plus sign (+), and select the protocol from which to redistribute routes into OSPF.
   f. Specify the name of a route policy to apply to the routes being redistributed. This name is one that you configured with a **policy route-policy** command.
   g. Click **Save**.
9. Click **Save** (for a new template) or **Update** (for an existing template).

## Configure Localized Control Policy Using CLI

To configure a route policy using the CLI:

1. Create lists of prefixes, as needed:
   ```
   vEdge(config)# policy
   vEdge(config-policy)# lists
   vEdge(config-lists)# prefix-list list-name
   vEdge(config-lists-list-name)# ip-prefix prefix/length
   ```

2. Create lists of BGP AS paths, and community and extended community attributes, as needed:
   ```
   vEdge(config)# policy lists
   vEdge(config-lists)# as-path-list list-name
   vEdge(config-lists-list-name)# as-path path-list
   vEdge(config)# policy lists
   vEdge(config-lists)# community-list list-name
   vEdge(config-lists-list-name)# community [internet | local-as | no-advertise | no-export]
   vEdge(config-lists)# ext-community-list list-name
   vEdge(config-lists-list-name)# community [rt (aa:nn | ip-address) | soo (aa:nn | ip-address)]
   ```

1. Create a route policy instance:
   ```
   vEdge(config)# policy route-policy policy-name
   vEdge(config-route-policy-policy-name)#
   ```

2. Create a series of match–action pair sequences:
   ```
   vEdge(config-route-policy-policy-name)# sequence number
   vEdge(config-sequence-number)#
   ```

   The match–action pairs are evaluated in order, by sequence number, starting with the lowest numbered pair and ending when the route matches the conditions in one of the pairs. Or if no match occurs, the default action is taken (either rejecting the route or accepting it as is).

3. Define match parameters for routes:
   ```
   vEdge(config-sequence-number)# match match-parameter
   ```

4. Define actions to take when a match occurs:
   ```
   vEdge(config-sequence-number)# action reject
   vEdge(config-sequence-number)# action accept set parameter
   ```

5. Create additional numbered sequences of match–action pairs within the router policy, as needed.

6. If a route does not match any of the conditions in one of the sequences, it is rejected by default. To accept nonmatching routes, configure the default action for the policy:
   ```
   vEdge(config-policy-name)# default-action accept
   ```

7. Apply the policy to a BGP address family, to all OSPF inbound routes, or when redistributing OSPF routes:
   ```
   vEdge(config)# vpn vpn-id router bgp local-as-number neighbor address
   vEdge(config-neighbor)# address-family ipv4-unicast
   ```
Structural Components for Localized Control Policy

Following are the structural components required to configure localized control policy. Each one is explained in more detail in the sections below.

```
policy
  lists
    as-path-list list-name
    as-path path-list
    community-list list-name
    community [as:nn | internet | local-as | no-advertise | no-export]
    ext-community-list list-name
    community [rt (aa:nn | ip-address) | soo (aa:nn | ip-address)]
    prefix-list list-name
    ip-prefix prefix/length
  route-policy policy-name
  sequence number
  match
    match-parameters
  action
    reject
    accept
    set parameters
  default-action
    (accept | reject)
  vpn vpn-id router bgp local-as-number neighbor address
  address-family ipv4-unicast
  route-policy policy-name (in | out)
  vpn vpn-id router ospf
  route-policy policy-name in
  redistribute (bgp | connected | nat | omp | static) route-policy policy-name
```

Lists

Route policy uses the following types of lists to group related items. You configure lists under the `policy lists` command hierarchy on Cisco devices.
### Table 7:

<table>
<thead>
<tr>
<th>List Type</th>
<th>Description</th>
<th>vManage Configuration/ CLI Configuration Command</th>
</tr>
</thead>
</table>
| AS paths  | List of one or more BGP AS paths. You can write each AS as a single number or as a regular expression. To specify more than one AS in a single path, include the list in quotation marks (" "). To configure multiple AS paths in a single list, include multiple `as-path` options, specifying one AS path in each option. | Configuration > Policies > Localized Policy > Add Policy > Create Groups of Interest > AS Path  
Configuration > Policies > Custom Options > Localized Policy > Lists > AS Path  
as-path-list `list-name` `as-path path-list` |
| Communities| List of one of more BGP communities. In `community`, you can specify:  
- `aa:nn`: Autonomous system number and network number. Each number is a 2-byte value with a range from 1 to 65535.  
- `internet`: Routes in this community are advertised to the Internet community. This community comprises all BGP-speaking networking devices.  
- `local-as`: Routes in this community are not advertised outside the local AS.  
- `no-advertise`: Attach the NO_ADVERTISE community to routes. Routes in this community are not advertised to other BGP peers.  
- `no-export`: Attach the NO_EXPORT community to routes. Routes in this community are not advertised outside the local AS or outside a BGP confederation boundary. To configure multiple BGP communities in a single list, include multiple `community` options, specifying one community in each option. | Configuration > Policies > Localized Policy > Add Policy > Create Groups of Interest > Community  
Configuration > Policies > Custom Options > Localized Policy > Lists > Community  
community-list `list-name`  
community `[aa:nn | internet | local-as | no-advertise | no-export]` |
### Structural Components for Localized Control Policy

<table>
<thead>
<tr>
<th>List Type</th>
<th>Description</th>
<th>vManage Configuration/ CLI</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Extended communities</strong></td>
<td>List of one or more BGP extended communities. In <strong>community</strong>, you can specify:</td>
<td><strong>Configuration &gt; Policies &gt; Localized Policy &gt; Add Policy &gt; Create Groups of Interest &gt; Extended Community</strong></td>
</tr>
<tr>
<td></td>
<td>• **rt (aa:nn</td>
<td>ip-address)**: Route target community, which is one or more routers that can receive a set of routes carried by BGP. Specify this as the autonomous system number and network number, where each number is a 2-byte value with a range from 1 to 65535, or as an IP address.</td>
</tr>
<tr>
<td></td>
<td>• **soo (aa:nn</td>
<td>ip-address)**: Route origin community, which is one or more routers that can inject a set of routes into BGP. Specify this as the autonomous system number and network number, where each number is a 2-byte value with a range from 1 to 65535, or as an IP address. To configure multiple extended BGP communities in a single list, include multiple <strong>community</strong> options, specifying one community in each option.</td>
</tr>
<tr>
<td><strong>Prefixes</strong></td>
<td>List of one or more IP prefixes. To configure multiple prefixes in a single list, include multiple <strong>ip-prefix</strong> options, specifying one prefix in each option. Specify the IP prefixes as follows:</td>
<td><strong>Configuration &gt; Policies &gt; Localized Policy &gt; Add Policy &gt; Create Groups of Interest &gt; Prefix</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>prefix/length</strong>—Exactly match a single prefix–length pair.</td>
<td><strong>Configuration &gt; Policies &gt; Custom Options &gt; Localized Policy &gt; Lists &gt; Prefix</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>0.0.0.0/0</strong>—Match any prefix–length pair.</td>
<td><strong>prefix-list list-name ip-prefix prefix/length</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>0.0.0.0/0 le length</strong>—Match any IP prefix whose length is less than or equal to <strong>length</strong>. For example, <strong>ip-prefix 0.0.0.0/0 le 16</strong> matches all IP prefixes with lengths from /1 through /16.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>0.0.0.0/0 ge length</strong>—Match any IP prefix whose length is greater than or equal to <strong>length</strong>. For example, <strong>ip-prefix 0.0.0.0 ge 25</strong> matches all IP prefixes with lengths from /25 through /32.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>0.0.0.0/0 ge length1 le length2</strong>, or <strong>0.0.0.0 le length2 ge length1</strong>—Match any IP prefix whose length is greater than or equal to <strong>length1</strong> and less than or equal to <strong>length2</strong>. For example, <strong>ip-prefix 0.0.0.0/0 ge 20 le 24</strong> matches all /20, /21, /22, /23, and /24 prefixes. Also, <strong>ip-prefix 0.0.0.0/0 le 24 ge 20</strong> matches the same prefixes. If <strong>length1</strong> and <strong>length2</strong> are the same, a single IP prefix length is matched. For example, <strong>ip-prefix 0.0.0.0/0 ge 24 le 24</strong> matches only /24 prefixes.</td>
<td></td>
</tr>
</tbody>
</table>

### Sequences

A localized control policy contains sequences of match–action pairs. The sequences are numbered to set the order in which a route is analyzed by the match–action pairs in the policy.
In the Cisco vManage NMS, you configure sequences from:

- Configuration > Policies > Localized Policy > Add Policy > Configure Route Policy > Sequence Type
- Configuration > Policies > Custom Options > Localized Policy > Route Policy > Sequence Type

In the CLI, you configure sequences with the `route-policy sequence` command.

Each sequence in a localized control policy can contain one match condition and one action condition.

**Match Parameters**

In the Cisco vManage NMS, you configure sequences from:

- Configuration > Policies > Localized Policy > Add Policy > Configure Route Policy > Sequence Type > Sequence Rule > Match
- Configuration > Policies > Custom Options > Localized Policy > Route Policy > Sequence Type > Sequence Rule > Match

In the CLI, you configure sequences with the `route-policy sequence match` command.

For route policy routes, you can match these attributes:

**Table 8:**

<table>
<thead>
<tr>
<th>Description</th>
<th>vManage Configuration/CLI Configuration Command</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP prefix or prefixes from which the route was learned</td>
<td>Match Address</td>
<td>Name of an IP prefix list</td>
</tr>
<tr>
<td></td>
<td>address list-name</td>
<td></td>
</tr>
<tr>
<td>BGP AS paths</td>
<td>Match AS Path List</td>
<td>Name of an AS path list</td>
</tr>
<tr>
<td></td>
<td>as-path list-name</td>
<td></td>
</tr>
<tr>
<td>BGP communities</td>
<td>Match Community List</td>
<td>Name of a BGP community list</td>
</tr>
<tr>
<td></td>
<td>community list-name</td>
<td></td>
</tr>
<tr>
<td>BGP extended communities</td>
<td>Match Extended Community List</td>
<td>Name of a BGP extended community list</td>
</tr>
<tr>
<td></td>
<td>ext-community list-name</td>
<td></td>
</tr>
<tr>
<td>BGP local preference</td>
<td>Match BGP Local Preference</td>
<td>0 through 4294967295</td>
</tr>
<tr>
<td></td>
<td>local-preference number</td>
<td></td>
</tr>
<tr>
<td>Route metric</td>
<td>Match Metric</td>
<td>0 through 4294967295</td>
</tr>
<tr>
<td></td>
<td>metric number</td>
<td></td>
</tr>
<tr>
<td>Next hop</td>
<td>Match Next Hop</td>
<td>Name of an IP prefix list</td>
</tr>
<tr>
<td></td>
<td>next-hop list-name</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>vManage Configuration/ CLI Configuration Command</td>
<td>Value or Range</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>OMP tag for OSPF</td>
<td>Match OMP Tag <code>omp-tag number</code></td>
<td>0 through 4294967295</td>
</tr>
<tr>
<td>BGP origin code</td>
<td>Match Origin <code>origin origin</code></td>
<td><code>egp</code> (default), <code>igp</code>, <code>incomplete</code></td>
</tr>
<tr>
<td>OSPF tag value</td>
<td>Match OSPF Tag <code>ospf-tag number</code></td>
<td>0 through 4294967295</td>
</tr>
<tr>
<td>Peer address</td>
<td>Match Peer <code>peer address</code></td>
<td>IP address</td>
</tr>
</tbody>
</table>

**Action Parameters**

For each match condition, you configure a corresponding action to take if the packet matches.

In the Cisco vManage NMS, you configure match parameters from:

- Configuration > Policies > Localized Policy > Add Policy > Configure Route Policy > Sequence Type > Sequence Rule > Action
- Configuration > Policies > Custom Options > Localized Policy > Configure Route Policy > Sequence Type > Sequence Rule > Action

In the CLI, you configure actions with the `policy control-policy action` command.

Each sequence in a localized control policy can contain one action condition.

When a route matches the conditions in the match portion of a route policy, the route can be accepted or rejected:

<table>
<thead>
<tr>
<th>Description</th>
<th>vManage Configuration/ CLI Configuration Command</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept the route. An accepted route is eligible to be modified by the additional parameters configured in the action portion of the policy configuration.</td>
<td>Click Accept <code>accept</code></td>
<td>—</td>
</tr>
<tr>
<td>Discard the packet.</td>
<td>Click Reject <code>reject</code></td>
<td>—</td>
</tr>
</tbody>
</table>

Then, for a route that is accepted, the following actions can be configured:
Table 10:

<table>
<thead>
<tr>
<th>Description</th>
<th>vManage Configuration/ CLI Configuration Command</th>
<th>Value or Range</th>
</tr>
</thead>
</table>
| Set the AS number in which a BGP route aggregator is located and the IP address of the route aggregator. | Click Accept, then action Aggregator
|                                                                              | set aggregator as-number ip-address                                                    | 1 through 65535                     |
| Set an AS number or a series of AS numbers to exclude from the AS path or to prepend to the AS path.   | Click Accept, then action AS Path
|                                                                              | set as-path (exclude | prepend) as-number                  | 1 through 65535                     |
| Set the BGP atomic aggregate attribute.                                     | Click Accept, then action Atomic Aggregate
|                                                                              | set atomic-aggregate                                                                | —                                   |
| Set the BGP community value.                                                | Click Accept, then action Community
|                                                                              | set community value                                                                  | [aa:nn | internet | local-as | no-advertise | no-export] |
| Set the BGP local preference.                                               | Click Accept, then action Local Preference
|                                                                              | set local-preference number                                                           | 0 through 429467295                 |
| Set the metric value.                                                       | Click Accept, then action Metric
|                                                                              | set metric number                                                                     | 0 through 429467295                 |
| Set the metric type.                                                        | Click Accept, then action Metric Type
|                                                                              | set metric-type type                                                                 | type1, type2                        |
| Set the next-hop address.                                                   | Click Accept, then action Next Hop
|                                                                              | set next-hop ip-address                                                               | IP address                          |
| Set the OMP tag for OSPF to use.                                           | Click Accept, then action OMP Tag
|                                                                              | set omp-tag number                                                                     | 0 through 429467295                 |
| Set the BGP origin code.                                                    | Click Accept, then action Origin
|                                                                              | set origin origin                                                                     | egp, igp (default), incomplete       |
| Set the IP address from which the route was learned.                       | Click Accept, then action Originator
|                                                                              | set originator ip-address                                                              | IP address                          |
| Set the OSPF tag value.                                                     | Click Accept, then action OSPF Tag
|                                                                              | set ospf-tag number                                                                    | 0 through 429467295                 |
| Set the BGP weight.                                                        | Click Accept, then action Weight
|                                                                              | set weight number                                                                      | 0 through 429467295                 |

To display the OMP and OSPF tag values associated with a route, use the `show ip routes detail` command.
**Action Parameters**

For each match condition, you configure a corresponding action to take if the packet matches.

In the Cisco vManage NMS, you configure match parameters from:

- **Configuration > Policies > Localized Policy > Add Policy > Configure Route Policy > Sequence Type > Sequence Rule > Action**

- **Configuration > Policies > Custom Options > Localized Policy > Configure Route Policy > Sequence Type > Sequence Rule > Action**

In the CLI, you configure actions with the `policy control-policy action` command.

Each sequence in a localized control policy can contain one action condition.

When a route matches the conditions in the match portion of a route policy, the route can be accepted or rejected:

**Table 11:**

<table>
<thead>
<tr>
<th>Description</th>
<th>vManage Configuration/ CLI Configuration Command</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept the route. An accepted route is eligible to be modified by the additional parameters configured in the action portion of the policy configuration.</td>
<td>Click Accept accept</td>
<td>—</td>
</tr>
<tr>
<td>Discard the packet.</td>
<td>Click Reject reject</td>
<td>—</td>
</tr>
</tbody>
</table>

Then, for a route that is accepted, the following actions can be configured:

**Table 12:**

<table>
<thead>
<tr>
<th>Description</th>
<th>vManage Configuration/ CLI Configuration Command</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the AS number in which a BGP route aggregator is located and the IP address of the route aggregator.</td>
<td>Click Accept, then action Aggregator <code>set aggregator as-number ip-address</code></td>
<td>1 through 65535</td>
</tr>
<tr>
<td>Set an AS number or a series of AS numbers to exclude from the AS path or to prepend to the AS path.</td>
<td>Click Accept, then action AS Path `set as-path (exclude</td>
<td>prepend) as-number`</td>
</tr>
<tr>
<td>Set the BGP atomic aggregate attribute.</td>
<td>Click Accept, then action Atomic Aggregate <code>set atomic-aggregate</code></td>
<td>—</td>
</tr>
<tr>
<td>Set the BGP community value.</td>
<td>Click Accept, then action Community <code>set community value</code></td>
<td>`[aa:nn</td>
</tr>
<tr>
<td>Set the BGP local preference.</td>
<td>Click Accept, then action Local Preference <code>set local-preference number</code></td>
<td>0 through 4294967295</td>
</tr>
<tr>
<td>Description</td>
<td>vManage Configuration/ CLI Configuration Command</td>
<td>Value or Range</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Set the metric value.</td>
<td>Click Accept, then action Metric set metric number</td>
<td>0 through 4294967295</td>
</tr>
<tr>
<td>Set the metric type.</td>
<td>Click Accept, then action Metric Type set metric-type type</td>
<td>type1, type2</td>
</tr>
<tr>
<td>Set the next-hop address.</td>
<td>Click Accept, then action Next Hop set next-hop ip-address</td>
<td>IP address</td>
</tr>
<tr>
<td>Set the OMP tag for OSPF to use.</td>
<td>Click Accept, then action OMP Tag set omp-tag number</td>
<td>0 through 4294967295</td>
</tr>
<tr>
<td>Set the BGP origin code.</td>
<td>Click Accept, then action Origin set origin origin</td>
<td>egp, igp (default), incomplete</td>
</tr>
<tr>
<td>Set the IP address from which the route was learned.</td>
<td>Click Accept, then action Originator set originator ip-address</td>
<td>IP address</td>
</tr>
<tr>
<td>Set the OSPF tag value.</td>
<td>Click Accept, then action OSPF Tag set ospf-tag number</td>
<td>0 through 4294967295</td>
</tr>
<tr>
<td>Set the BGP weight.</td>
<td>Click Accept, then action Weight set weight number</td>
<td>0 through 4294967295</td>
</tr>
</tbody>
</table>

To display the OMP and OSPF tag values associated with a route, use the `show ip routes detail` command.

**Default Action**

If a route being evaluated does not match any of the match conditions in a localized control policy, a default action is applied to this route. By default, the route is rejected.

In the Cisco vManage NMS, you modify the default action from Configuration > Policies > Localized Policy > Add Policy > Configure Route Policy > Sequence Type > Sequence Rule > Default > Action.

In the CLI, you modify the default action with the `control policy default-action accept` command.

**Apply Route Policy for BGP**

For a route policy to take effect for BGP, you must apply it to an address family. Currently, the Cisco SD-WAN software supports only the IPv4 address family.

To apply a BGP route policy in the Cisco vManage NMS:

1. In the Cisco vManage NMS, select the Configure > Templates screen.
2. In the Device tab, click the Create Template drop-down and select From Feature Template.
3. From the Device Model drop-down, select the type of device for which you are creating the template. The Cisco vManage NMS displays all the feature templates for that device type. The required feature templates are indicated with an asterisk (*), and the remaining templates are optional. The factory-default template for each feature is selected by default.

4. In the Template Name field, enter a name for the device template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.

5. In the Description field, enter a description for the device template. This field is mandatory, and it can contain any characters and spaces.

6. In the Basic Information bar, click the Service VPN tab.

7. In the Service VPN field, select the VPN number.

8. In Additional VPN Templates, select BGP.

9. Select Create Template.

10. In the Basic Configuration bar, click IPv4 Unicast Address Family.

11. In the Address Family field, select ipv4-unicast.

12. In the Redistribute tab, click New Redistribute.

13. In the Route Policy field, enter the name of the route policy to apply to redistributed routes.

14. Click Add.

15. Click Save.

To apply a BGP route policy in the CLI:

```
Device(config)# vpn
vpn-id
router bgp
local-as-number
neighbor address
address-family ipv4-unicast route-policy
policy-name (in | out)
```

Applying the policy in the inbound direction (in) affects routes being received by BGP. Applying the policy in the outbound direction (out) affects routes being advertised by BGP.

**Apply Route Policy for OSPF**

For a route policy to take effect for OSPF, you can apply it to all inbound traffic.

To apply an OSPF route policy in the Cisco vManage NMS:

1. In the Cisco vManage NMS, select the Configure > Templates screen.

2. In the Device tab, click the Create Template drop-down and select From Feature Template.

3. From the Device Model drop-down, select the type of device for which you are creating the template. The Cisco vManage NMS displays all the feature templates for that device type. The required feature templates are indicated with an asterisk (*), and the remaining templates are optional. The factory-default template for each feature is selected by default.
4. In the Template Name field, enter a name for the device template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.

5. In the Description field, enter a description for the device template. This field is mandatory, and it can contain any characters and spaces.

6. In the Basic Information bar, click the Service VPN tab.

7. In the Service VPN field, select the VPN number.

8. In Additional VPN Templates, select OSPF.

9. Select Create Template.

10. In the Basic Configuration bar, click Redistribute.

11. Click New Redistribute.

12. In the Route Policy field, enter the name of the route policy to apply to redistributed routes.

13. Click Add.

14. Click Save.

To apply an OSPF route policy in the CLI:

```
Device(config)# vpn vpn-id
router ospf route-policy policy-name in
```

You can also apply the policy when redistributing routes into OSPF:

```
Device(config)# vpn
vpn-id
router ospf redistribute (bgp|connected|nat|omp|static) route-policy
policy-name
```

### Device Access Policy

#### Device Acess Policy

**Table 13: Feature History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco SD-WAN 19.3</td>
<td>Feature introduced. This feature defines the rules that traffic must meet to pass through an interface. When you define rules for incoming traffic, they are applied to the traffic before any other policies are applied. Cisco XE SD-WAN device control plane process the data traffic for local services (like SSH and SNMP) from a set of sources in a VPN. Routing packets are required to form the overlay. It is important to protect the control plane CPU from device access traffic by applying the filter.</td>
</tr>
</tbody>
</table>
Device Access Policy Overview

The Cisco vManage user interface is enhanced to configure device access policy on Cisco vEdge devices. Cisco vEdge device control plane processes the data traffic for local services (like SSH and SNMP) from a set of sources in a VPN. It is important to protect the control plane CPU from device access traffic by applying the filter.

Access policies define the rules that traffic must meet to pass through an interface. When you define rules for incoming traffic, they are applied to the traffic before any other policies are applied. You can use access policies, or rules, in routed and transparent firewall mode to control IP traffic. An access rule permits or denies traffic based on the protocol, a source and destination IP address or network, and optionally, the users and the user groups. Each packet that arrives at an interface is examined to determine whether to forward or drop the packet based on criteria you specify. If you define access rules for the outgoing traffic, packets are also analyzed before they are allowed to leave an interface. Access policies are applied in order. That is, when the device compares a packet to the rules, it searches from top to bottom in the access policies list, and applies the policy for the first matched rule, ignoring all subsequent rules (even if a later rule is a better match). Thus, you should place specific rules above more general rules to ensure those rules are not skipped.

Configure Device Access Policy Using vManage

Cisco vEdge device supports device access policy configuration to handle SNMP and SSH traffic directed towards Control Plane. Cisco vManage configures destination port based on device access policy.

To configure localized device access control policies, use the Cisco vManage policy configuration wizard. Configure some or all these components depending on the specific policy you are creating. To skip a component, click the Next button. To return to a component, click the Back button at the bottom of the screen.

To configure Device Access Policy:

1. In the Cisco vManage, select the Configure > Policies screen.
2. Select the Localized Policy tab.
3. From Custom Options > Localized Policy pane, select Access Control Lists.
4. Click Add Device Access Policy drop down list to add a device. The options are Add IPv4 Device Access Policy and Add IPv6 Device Access Policy.
5. Select Add IPv4 Device Access Policy from the drop-down list to add IPv4 ACL Policy.
   The Edit Device IPv4 ACL Policy page displays.
6. Enter the name and the description for the new policy.
7. Click Add ACL Sequence to add a sequence.
8. Click Sequence Rule. Match and Actions options display.
9. From the Match pane, select and configure the following conditions for your ACL policy:

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Access Protocol (required)</td>
<td>Select a carrier from the drop-down list. For example SNMP, SSH.</td>
</tr>
<tr>
<td>Source Data Prefix</td>
<td>Enter the source IP address. For example, 10.0.0.0/12.</td>
</tr>
<tr>
<td>Match Condition</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Source Port</td>
<td>Enter the list of source ports. The range is 0-65535.</td>
</tr>
<tr>
<td>Destination Data Prefix</td>
<td>Enter the destination IP address. For example, 10.0.0.0/12.</td>
</tr>
<tr>
<td>Destination VPN</td>
<td>Enter the list of VPN ID.</td>
</tr>
</tbody>
</table>

10. From the **Actions** tab, configure the following conditions for your ACL policy:

<table>
<thead>
<tr>
<th>Action Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept</td>
<td>Enter the counter name. The maximum length can be 20 characters.</td>
</tr>
<tr>
<td>Counter Name</td>
<td>Enter the counter name. The maximum length can be 20 characters.</td>
</tr>
</tbody>
</table>

11. Click **Save Match And Actions** to save all the conditions for ACL policy.

12. Click **Save Device Access Control List Policy** to apply the selected match conditions to an action.

13. If no packets match any of the route policy sequence rules, the **Default Action** in the left pane is to drop the packets.

---

**Note**

IPv6 Prefix match is not supported on Cisco vEdge devices. When you try to configure IPv6 prefix match on the Cisco vEdge device, Cisco vManage fails to generate device configuration.

---

**Configure Device Access Policy Using CLIs**

To configure Device Access Policy:

```
Device(config)# system
Device(config-system) device-access-policy ipv4 <pol-name>
```

```
Device(config)# policy
Device(config-policy) policy device-access-policy <name>
```

Sample Configuration:

```
Device(config)# policy
Device(config-policy) policy device-access-policy <name>
sequence 1
    match
        destination-data-prefix-list Destination prefix list
        destination-ip List of destination addresses
        destination-port List of destination ports
        dscp List of DSCP values
```
IPv6 Prefix match is not supported on Cisco vEdge devices.

The following example shows the sample configuration for Device Access Policy:

```
policy device-access-policy dev_pol
  sequence 1
    match
      destination-port 22
    !
    action drop
    count ssh_packs
    !
    default-action drop
    !
    device-access-policy snmp_policy
  sequence 2
    match
      destination-port 161
    !
    action drop
    count snmp_packs
    !
    default-action accept
    !
  system
  device-access-policy ipv4 snmp_policy
```

**Verifying Device Access Policy Configuration**

Cisco vEdge devices support the following operational commands to provide information for device-access-policy. These commands provide a visual for the counters and the names of the configured device-access-policy. The two commands and the respective yang models are shown in the following sections.

**Yang Model for the command `device-access-policy-counters`:**

```
list device-access-policy-counters {
  tailf:info "IPv6 Device Access Policy counters";
  when "/viptela-system:system/viptela-system:personality = 'vedge'";
  tailf:callpoint device-access-policy-counters-v6; // _nfvis_exclude_line_
    key "name";
```
Verifying Device Access Policy Configuration

Command

show policy device-access-policy-counters

Output:

<table>
<thead>
<tr>
<th>NAME</th>
<th>NAME</th>
<th>PACKETS</th>
<th>BYTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>dev_pol</td>
<td>ssh_packs</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>snmp_policy</td>
<td>snmp_packs</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Yang Model for the command `device-access-policy-names`:

list device-access-policy-names {
  tailf:info "IPv6 device access policy names";
  when "/viptela-system:system/viptela-system:personality = 'vedge'";
  tailf:callpoint device-access-policy-names-v6; // _nfvis_exclude_line_
  tailf:cli-no-key-completion;
  key "name";
  tailf:hidden cli;

  leaf name {
    tailf:info "Device Access Policy name";
    type viptela:named-type-127;
  }
  config false;
}

Command

show policy device-access-policy-names
Output:

NAME
-------------
dev_pol
snmp_policy
Data Policies

Data policy influences the flow of data traffic traversing the network based either on fields in the IP header of packets or the router interface on which the traffic is being transmitted or received. Data traffic travels over the IPsec connections between Cisco devices, shown in purple in the adjacent figure.

The Cisco SD-WAN architecture implements two types of data policy:

- Centralized data policy controls the flow of data traffic based on the source and destination addresses and ports and DSCP fields in the packet's IP header (referred to as a 5-tuple), and based on network segmentation and VPN membership. These types of data policy are provisioned centrally, on the Cisco vSmart Controller, and they affect traffic flow across the entire network.

- Localized data policy controls the flow of data traffic into and out of interfaces and interface queues on Cisco devices. This type of data policy is provisioned locally, on the Cisco devices, using access lists. It allows you to classify traffic and map different classes to different queues. It also allows you to mirror traffic and to police the rate at which data traffic is transmitted and received.

By default, no centralized data policy is provisioned. The result is that all prefixes within a VPN are reachable from anywhere in the VPN. Provisioning centralized data policy allows you to apply a 6-tuple filter that controls access between sources and destinations.
As with centralized control policy, you provision centralized data policy on the Cisco vSmart Controller, and that configuration remains on the Cisco vSmart Controller. The effects of data policy are reflected in how the Cisco devices direct data traffic to its destination. Unlike control policy, however, centralized data policies are pushed to the Cisco devices in a read-only fashion. They are not added to the device's configuration file, but you can view them from the CLI on the device.

With no access lists provisioned on Cisco devices, all data traffic is transmitted at line rate and with equal importance, using one of the interface's queues. Using access lists, you can provision class of service, which allows you to classify data traffic by importance, spread it across different interface queues, and control the rate at which different classes of traffic are transmitted. You can also provision policing and packet mirroring.

The `show sdwan policy data-policy-filter` commands display in different formats depending on if the counter has a value or not. If the counter has a value, the output for the `show sdwan policy data-policy-filter` command displays in a linear format. If the counter does not have a value, the output displays in a tabular format.

**Centralized Data Policy**

Centralized data policy is policy that is configured on a Cisco vSmart Controller (hence, it is centralized) and that affects data traffic being transmitted between the routers on the Cisco SD-WAN overlay network.

**Centralized Data Policy Overview**

Data policy operates on the data plane in the Cisco SD-WAN overlay network and affects how data traffic is sent among the Cisco devices in the network. The Cisco SD-WAN architecture defines two types of data policy, centralized data policy, which controls the flow of data traffic based on the IP header fields in the data packets and based on network segmentation, and localized data policy, which controls the flow of data traffic into and out of interfaces and interface queues on Cisco devices.

Centralized data policy is applied to packets that originate from a specific sender, or source address, for instance, from a workstation in a local site that is sending voice, data, or other traffic, and it controls which destinations within a VPN the traffic can reach. Data policy is applied to data traffic based on a 6-tuple of fields in the packet's IP header: source IP address, source port, destination IP address, destination port, DSCP, and protocol.
As with control policy, data policy is provisioned centrally on a Cisco vSmart Controller and is applied only on the Cisco vSmart Controller controller. The data policy itself is never pushed to the Cisco devices in the network. What is pushed to the Cisco devices, via OMP and based on the site ID, are the results of the data policy; hence, the effects of the policy are reflected on the Cisco devices. Normally, the data policy on a Cisco device acts as the data policy for the entire site that sits behind the device. Data policy that comes from the Cisco vSmart Controller is always implicitly applied in the inbound direction.

Data policy can be applied to data traffic based on the packet header fields, such as the prefix, port, protocol, and DSCP value, and they can also be applied based on the VPN in the overlay network to which the traffic flows.

**Data Policy Based on Packet Header Fields**

Policy decisions affecting data traffic can be based on the packet header fields, specifically, on the source and destination IP prefixes, the source and destination IP ports, the protocol, and the DSCP.

This type of policy is often used to modify traffic flow in the network. Here are some examples of the types of control that can be effected with centralized data policy:

- Which set of sources are allowed to send traffic to any destination outside the local site. For example, local sources that are rejected by such a data policy can communicate only with hosts on the local network.
- Which set of sources are allowed to send traffic to a specific set of destinations outside the local site. For example, local sources that match this type of data policy can send voice traffic over one path and data traffic over another.
- Which source addresses and source ports are allowed to send traffic to any destination outside the local site or to a specific port at a specific destination.

**Deep Packet Inspection**

In addition to examining the network- and transport-layer headers in data packets, centralized data policy can be used to examine the application information in the data packets’ payload. This deep packet inspection offers control over how data packets from specific applications or application families are forwarded across the network, allowing you to assign the traffic to be carried by specific tunnels. To control the traffic flow of specific application traffic based on the traffic loss or latency properties on a tunnel, use application-aware routing.

To base policy decisions on source and destination prefixes and on the headers in the IP data packets, you use centralized data policy, which you configure with the `policy data-policy` command. The Cisco vSmart Controller pushes this type of data policy to the Cisco devices. In domains with multiple Cisco vSmart Controllers, all the controllers must have the same centralized data policy configuration to ensure that traffic flow within the overlay network remains synchronized.

To base policy decisions on the application information in the packet payload, you use centralized data policy to perform deep packet inspection. You configure this by creating lists of applications with the `policy lists app-list` command and then calling these lists in a `policy data-policy` command.

To specify the path that application traffic takes through the network, you can set the local TLOC or the remote TLOC, or both, to use to send the traffic over.

To configure the VPNs that Cisco devices are allowed to receive routes from, you use centralized data policy, which you configure with the `policy vpn-membership` command. VPN membership policy affects which routes the Cisco vSmart Controller sends to the Cisco devices. The policy itself remains on the Cisco vSmart Controller and is not pushed to the Cisco devices.
Configure Centralized Data Policy Based on Prefixes and IP Headers

A centralized data policy based on source and destination prefixes and on headers in IP packets consists of a series of numbered (ordered) sequences of match-action pairs that are evaluated in order, from lowest sequence number to highest sequence number. When a packet matches one of the match conditions, the associated action is taken and policy evaluation on that packet stops. Keep this in mind as you design your policies to ensure that the desired actions are taken on the items subject to policy.

If a packet matches no parameters in any of the sequences in the policy configuration, it is dropped and discarded by default.

Configuration Components

The following figure illustrates the configuration components for centralized data policy:

To configure centralized data policies, use the Cisco vManage policy configuration wizard. The wizard consists of four sequential screens that guide you through the process of creating and editing policy components:

- **Create Groups of Interest**—Create lists that group together related items and that you call in the match or action components of a policy.
- **Configure Traffic Rules**—Create the match and action conditions of a policy.
- **Apply Policies to Sites and VPNs**—Associate policy with sites and VPNs in the overlay network.

In the first three policy configuration wizard screens, you are creating policy components or blocks. In the last screen, you are applying policy blocks to sites and VPNs in the overlay network.

For a centralized data policy to take effect, you must activate the policy.

This section provides general procedures for configuring centralized data policy on Cisco vSmart Controllers. Centralized data policy can be used for different purposes, which are described in the sections that follow.

Start the Policy Configuration Wizard

To start the policy configuration wizard:

**Step 1**  
In the Cisco vManage NMS, select the **Configure > Policies** screen.
Step 2: Select the Centralized Policy tab.

Step 3: Click Add Policy. The policy configuration wizard opens, and the Create Groups of Interest screen displays.

Step 1: Create Policy Lists

You can create lists of groups to use in centralized policy.

<table>
<thead>
<tr>
<th>List Type</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| Application | a. In the left bar, click Application.  
b. Click New Application List.  
c. Enter a name for the list.  
d. Click either the Application or Application Family button.  
e. From the Select drop-down, select the desired applications or application families.  
f. Click Add. |

Two application lists are preconfigured. You cannot edit or delete these lists.

- **Google Apps**—Includes Google applications, such as gmail, Google maps, and YouTube. To display a full list of Google applications, click the list in the Entries column.
- **Microsoft Apps**—Includes Microsoft applications, such as Excel, Skype, and Xbox. To display a full list of Microsoft applications, click the list in the Entries column.
### Step 1: Create Policy Lists

<table>
<thead>
<tr>
<th>List Type</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| **Color** | a. In the left bar, click **Color**.  
  b. Click **New Color List**.  
  The Color List popup displays.  
  c. Enter a name for the list  
  d. From the Select Color drop-down, select the desired colors.  
  e. Click **Add**. |
| **Data Prefix** | a. In the left bar, click **Data Prefix**.  
  b. Click **New Data Prefix List**.  
  c. Enter a name for the list.  
  d. In the Add Data Prefix field, enter one or more data prefixes separated by commas.  
  e. Click **Add**. |
| **Policer** | a. In the left bar, click **Policer**.  
  b. Click **New Policer List**.  
  c. Enter a name for the list.  
  d. Define the policing parameters:  
    1. In the Burst field, enter the maximum traffic burst size, a value from 15,000 to 10,000,000 bytes.  
    2. In the Exceed field, select the action to take when the burst size or traffic rate is exceeded. It can be drop, which sets the packet loss priority (PLP) to low.  
       You can use the remark action to set the packet loss priority (PLP) to high.  
    3. In the Rate field, enter the maximum traffic rate, a value from 0 through 2^{64} – 1 bits per second (bps).  
  e. Click **Add**. |
| **Prefix** | a. In the left bar, click **Prefix**.  
  b. Click **New Prefix List**.  
  c. Enter a name for the list.  
  d. In the Add Prefix field, enter one or more data prefixes separated by commas.  
  e. Click **Add**. |
<table>
<thead>
<tr>
<th>List Type</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| Site      | a. In the left bar, click **Site**.  
            b. Click **New Site List**.  
            c. Enter a name for the list.  
            d. In the Add Site field, enter one or more site IDs separated by commas.  
            e. Click **Add**. |
| SLA Class | a. In the left bar, click **SLA Class**.  
            b. Click **New SLA Class List**.  
            c. Enter a name for the list.  
            d. Define the SLA class parameters:  
               1. In the **Loss** field, enter the maximum packet loss on the connection, a value from 0 through 100 percent.  
               2. In the **Latency** field, enter the maximum packet latency on the connection, a value from 0 through 1,000 milliseconds.  
               3. In the **Jitter** field, enter the maximum jitter on the connection, a value from 1 through 1,000 milliseconds.  
            e. Click **Add**. |
| TLOC      | a. In the left bar, click **TLOC**.  
            b. Click **New TLOC List**. The TLOC List popup displays.  
            c. Enter a name for the list.  
            d. In the **TLOC IP** field, enter the system IP address for the TLOC.  
            e. In the **Color** field, select the TLOC's color.  
            f. In the **Encap** field, select the encapsulation type.  
            g. In the **Preference** field, optionally select a preference to associate with the TLOC.  
            h. Click **Add TLOC** to add another TLOC to the list.  
            i. Click **Save**. |
| VPN       | a. In the left bar, click **VPN**.  
            b. Click **New VPN List**.  
            c. Enter a name for the list.  
            d. In the **Add VPN** field, enter one or more VPN IDs separated by commas.  
            e. Click **Add**. |
Step 2: Configure Traffic Rules

When you first open the Traffic Rules screen, the Application-Aware Routing tab is selected by default. To configure traffic rules for deep packet inspection, see Deep Packet Inspection, on page 105.

To configure traffic rules for centralized data policy:

Step 1
Click the Traffic Data tab.

Step 2
Click the Add Policy drop-down.

Step 3
Click Create New. The Add Data Policy screen displays.

Step 4
Enter a name and description for the data policy.

Step 5
In the right pane, click Sequence Type. The Add Data Policy popup opens.

Step 6
Select the type of data policy you want to create. Choices are: Application Firewall, QoS, Service Chaining, Traffic Engineering, and Custom.

Step 7
A policy sequence containing the text string Application Firewall, QoS, Service Chaining, Traffic Engineering, or Custom is added in the left pane.

Step 8
Double-click the text string, and enter a name for the policy sequence. The name you type is displayed both in the Sequence Type list in the left pane and in the right pane.

Step 9
In the right pane, click Sequence Rule. The Match/Action box opens, and Match is selected by default. The available policy match conditions are listed below the box.

Step 10
For QoS and Traffic Engineering data policies: From the Protocol drop-down list, select IPv4 to apply the policy only to IPv4 address families.

Step 11
To select one or more Match conditions, click its box and set the values as described in the following table. Note that not all match conditions are available for all policy sequence types.

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Procedure</th>
<th>IPv4 Fields</th>
<th>IPv6 Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>None (match all packets)</td>
<td>Do not specify any match conditions.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Match Condition</td>
<td>Procedure</td>
<td>IPv4 Fields</td>
<td>IPv6 Fields</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------</td>
<td>-------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Applications / Application Family List | a. In the Match conditions, click **Applications/Application Family List**.  
  b. In the drop-down, select the application family.  
  c. To create an application list:  
    1. Click **New Application List**.  
    2. Enter a name for the list.  
    3. Click **Application** to create a list of individual applications. Click **Application Family** to create a list of related applications.  
    4. In the **Select Application** drop-down, select the desired applications or application families.  
    5. Click **Save**. | | app-list |
| Destination Data Prefix | a. In the Match conditions, click **Destination Data Prefix**.  
  b. To match a list of destination prefixes, select the list from the drop-down.  
  c. To match an individual destination prefix, enter the prefix in the **Destination: IP Prefix** field. | source/destination-data-prefix-list | source/destination-data-prefix-list |
| Destination Port | a. In the Match conditions, click **Destination Port**.  
  b. In the **Destination: Port** field, enter the port number. Specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]). | src/dst ip | src/dst ip |
| DNS Application List | Add an application list to enable split DNS.  
  a. In the Match conditions, click **DNS Application List**.  
  b. In the drop-down, select the application family. | dns-app-list | |
| DNS | Add an application list to process split DNS.  
  a. In the Match conditions, click **DNS**.  
  b. In the drop-down, select **Request** to process DNS requests for the DNS applications, and select **Response** to process DNS responses for the applications. | dns-request  
dns-response | |
### Step 2: Configure Traffic Rules

#### Data Policies

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Procedure</th>
<th>IPv4 Fields</th>
<th>IPv6 Fields</th>
</tr>
</thead>
</table>
| **DSCP**        | a. In the Match conditions, click **DSCP**.  
                  b. In the **DSCP** field, type the DSCP value, a number from 0 through 63. | dscp | dscp |
| **Packet Length** | a. In the Match conditions, click **Packet Length**.  
                      b. In the Packet Length field, type the length, a value from 0 through 65535. | packet-len | packet-len |
| **PLP**         | a. In the Match conditions, click **PLP** to set the Packet Loss Priority.  
                    b. In the PLP drop-down, select **Low** or **High**. To set the PLP to high, apply a policer that includes the **exceed remark** option. |  |  |
| **Protocol**    | a. In the Match conditions, click **Protocol**.  
                    b. In the Protocol field, type the Internet Protocol number, a number from 0 through 255. | protocol | protocol/next header |
| **Source Data Prefix** | a. In the Match conditions, click **Source Data Prefix**.  
                            b. To match a list of source prefixes, select the list from the drop-down.  
                            c. To match an individual source prefix, enter the prefix in the **Source** field. | source/destination-data-prefix-list | source/destination-data-prefix-list |
| **Source Port** | a. In the Match conditions, click **Source Port**.  
                        b. In the Source field, enter the port number. Specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]). | ports | ports |
| **TCP**         | a. In the Match conditions, click **TCP**.  
                        b. In the TCP field, **syn** is the only option available. | tcp flag |  |

**Step 12** To select actions to take on matching data traffic, click the **Actions** box.

**Step 13** To drop matching traffic, click **Drop**. The available policy actions are listed to the right of the button.

**Step 14** To accept matching traffic, click **Accept**. The available policy actions are listed to the right of the button.

**Step 15** Set the policy action as described in the following table. Note that not all actions are available for all match conditions.
<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Description</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| **Counter**     | Count matching data packets. | a. In the Action conditions, click **Counter**.  
b. In the **Counter Name** field, enter the name of the file in which to store packet counters. |
| **DSCP**        | Assign a DSCP value to matching data packets. | a. In the Action conditions, click **DSCP**.  
b. In the **DSCP** field, type the DSCP value, a number from 0 through 63. |
| **Forwarding Class** | Assign a forwarding class to matching data packets. | a. In the Match conditions, click **Forwarding Class**.  
b. In the **Forwarding Class** field, type the class value, which can be up to 32 characters long. |
| **Log**         | Place a sampled set of packets that match the SLA class rule into system logging (syslog) files. In addition to logging the packet headers, a syslog message is generated the first time a packet header is logged and then every 5 minutes thereafter, as long as the flow is active. | a. In the Action conditions, click **Log** to enable logging. |
| **Policer**     | Apply a policer to matching data packets. | a. In the Match conditions, click **Policer**.  
b. In the Policер drop-down field, select the name of a policer. |
## Step 3: Apply Policies to Sites and VPNs

In Apply Policies to Sites and VPNs, apply a policy to overlay network sites and VPNs.

### Step 1
In the **Policy Name** field, enter a name for the policy. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (−), and underscores (_). It cannot contain spaces or any other characters.

### Step 2
In the **Policy Description** field, enter a description of the policy. It can contain up to 2048 characters. This field is mandatory, and it can contain any characters and spaces.

### Step 3
From the Topology bar, select the tab that corresponds to the type of policy block—**Topology**, **Application-Aware Routing**, **Traffic Data**, or **Cflowd**. The table then lists policies that you have created for that type of policy block.

### Step 4
Associate the policy with VPNs and sites. The choice of VPNs and sites depends on the type of policy block:

- a) For a **Topology** policy block, click **Add New Site List and VPN List** or **Add New Site**. Some topology blocks might have no **Add** buttons. Select one or more site lists, and select one or more VPN lists. Click **Add**.

- b) For an **Application-Aware Routing** policy block, click **Add New Site List and VPN List**. Select one or more site lists, and select one or more VPN lists. Click **Add**.
Step 4: Activate a Centralized Data Policy

Activating a centralized data policy sends that policy to all connected Cisco vSmart Controllers. To activate a centralized policy:

Step 1
In the Cisco vManage NMS, select the Configure > Policies screen.

Step 2
Select a policy from the policy table.

Step 3
Click the More Actions icon to the right of the row, and click Activate. The Activate Policy popup opens. It lists the IP addresses of the reachable Cisco vSmart Controllers to which the policy is to be applied.

Step 4
Click Activate.

Configure Centralized Data Policy Using CLI

Following are the high-level steps for configuring a VPN membership data policy:

1. Create a list of overlay network sites to which the VPN membership policy is to be applied (in the apply-policy command):

   ```
   vSmart(config)# policy
   vSmart (config-policy)# lists site-list list-name
   vSmart(config-lists-list-name)# site-id site-id
   ```

   The list can contain as many site IDs as necessary. Include one site-id command for each site ID. For contiguous site IDs, you can specify a range of numbers separated with a dash (–). Create additional site lists, as needed.

2. Create lists of IP prefixes and VPNs, as needed:

   ```
   vSmart(config)# policy lists
   vSmart(config-lists)# data-prefix-list list-name
   vSmart(config-lists-list-name)# ip-prefix prefix/length
   vSmart(config)# policy lists
   vSmart(config-lists)# vpn-list list-name
   vSmart(config-lists-list-name)# vpn vpn-id
   ```

3. Create lists of TLOCs, as needed.

   ```
   vSmart(config)# policy
   vSmart (config-policy)# lists tloc-list list-name
   vSmart(config-lists-list-name)# tloc ip-address color color encapsulation [preference number]
   ```

4. Define policing parameters, as needed:
5. Create a data policy instance and associate it with a list of VPNs:

```bash
vSmart(config)# policy data-policy policy-name
vSmart(config-data-policy-policy-name)# vpn-list list-name
```

6. Create a series of match–action sequences:

```bash
vSmart(config-vpn-list)# sequence number
vSmart(config-sequence-number)#
```

The match–action pairs are evaluated in order, by sequence number, starting with the lowest numbered pair and ending when the route matches the conditions in one of the pairs. Or if no match occurs, the default action is taken (either rejecting the route or accepting it as is).

7. Define match parameters for packets:

```bash
vSmart(config-sequence-number)# match parameters
```

8. Define actions to take when a match occurs:

```bash
vSmart(config-sequence-number)# action (accept | drop) [count counter-name] [log] [tcp-optimization]
vSmart(config-sequence-number)# action accept nat [pool number] [use-vpn 0]
vSmart(config-sequence-number)# action accept redirect-dns (host | ip-address)
vSmart(config-sequence-number)# action accept set parameters
```

9. Create additional numbered sequences of match–action pairs within the data policy, as needed.

10. If a route does not match any of the conditions in one of the sequences, it is rejected by default. To accept nonmatching prefixed, configure the default action for the policy:

```bash
vSmart(config-policy-name)# default-action accept
```

11. Apply the policy to one or more sites in the overlay network:

```bash
vSmart(config)# apply-policy site-list list-name data-policy policy-name {all | from-service | from-tunnel}
```

---

**Structural Components of Policy Configuration for Centralized Data Policy**

The following commands are the structural components required to configure VPN membership policy. Each one is explained in more detail in the sections that follow.

```bash
policy
lists
app-list list-name
  (app applications | app-family application-families)
data-prefix-list list-name
  ip-prefix prefix
site-list list-name
site-id site-id
tloc-list list-name
tloc ip-address color color encap encapsulation [preference value]
vpn-list list-name
  vpn vpn-id
policer policer-name
  burst bytes
  exceed action
```
Centralized data policy for deep packet inspection uses the following types of lists to group related items. In the CLI, you configure lists under the **policy lists** command hierarchy on Cisco vSmart Controllers.

- **Configuration > Policies > Centralized Policy > Add Policy > Create Groups of Interest**
- **Configuration > Policies > Custom Options > Lists.**

In the CLI, you configure lists under the **policy lists** command hierarchy on Cisco vSmart Controllers.
<table>
<thead>
<tr>
<th>List Type</th>
<th>Description</th>
<th>vManage / CLI Command</th>
</tr>
</thead>
</table>
| Applications and application families | List of one or more applications or application families running on the subnets connected to the Cisco device.  
  - *application-names* can be the names of one or more applications. The Cisco SD-WAN software supports about 2300 different applications. To list the supported applications, use the `?` in the CLI.  
  - *application-families* can be one or more of the following: antivirus, application-service, audio_video, authentication, behavioral, compression, database, encrypted, erp, file-server, file-transfer, forum, game, instant-messaging, mail, microsoft-office, middleware, network-management, network-service, peer-to-peer, printer, routing, security-service, standard, telephony, terminal, thin-client, tunneling, wap, web, and webmail. | Configuration > Policies > Centralized Policy > Add Policy > Create Groups of Interest > Application  
  or  
  Configuration > Policies > Centralized Policy > Lists > Application  
  `app-list list-name`  
  `(app applications | app-family application-families)` |
| Prefixes                        | List of one or more IP prefixes.                                                                                                                                                                             | Configuration > Policies > Centralized Policy > Add Policy > Create Groups of Interest > Prefix  
  or  
  Configuration > Policies > Custom Options > Centralized Policy > Lists > Prefix  
  `prefix-list list-name`  
  `ip-prefix prefix/length` |
<table>
<thead>
<tr>
<th>List Type</th>
<th>Description</th>
<th>vManage / CLI Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sites</td>
<td>List of one or more site identifiers in the overlay network. You can specify a single site identifier (such as <code>site-id 1</code>) or a range of site identifiers (such as <code>site-id 1-10</code>).</td>
<td>Configuration &gt; Policies &gt; Centralized Policy &gt; Add Policy &gt; Create Groups of Interest &gt; Site or Configuration &gt; Policies &gt; Custom Options &gt; Centralized Policy &gt; Lists &gt; Site <code>site-list list-name</code> <code>site-id site-id</code></td>
</tr>
<tr>
<td>TLOCs</td>
<td>List of one or more TLOCs in the overlay network. For each TLOC, specify its address, color, and encapsulation. <code>address</code> is the system IP address. <code>color</code> can be one of <code>3g, biz-internet, blue, bronze, custom1, custom2, custom3, default, gold, green, lte, metro-ethernet, mpls, mpls-restricted, privatel through private6, public-internet, red, and silver</code>. Encapsulation can be <code>gre</code> or <code>ipsec</code>. Optionally, set a preference value (from 0 to 232 – 1) to associate with the TLOC address. When you apply a TLOC list in an action <code>accept</code> condition, when multiple TLOCs are available and satisfy the match conditions, the TLOC with the lowest preference value is used. If two or more of TLOCs have the lowest preference value, traffic is sent among them in an ECMP fashion.</td>
<td>Configuration &gt; Policies &gt; Centralized Policy &gt; Add Policy &gt; Create Groups of Interest &gt; TLOC or Configuration &gt; Policies &gt; Custom Options &gt; Centralized Policy &gt; Lists &gt; Site <code>tloc-list list-name</code> <code>tloc ip-address color color encapsulation [preference number]</code></td>
</tr>
<tr>
<td>VPNs</td>
<td>List of one or more VPNs in the overlay network. For data policy, you can configure any VPNs except for VPN 0 and VPN 512. To configure multiple VPNs in a single list, include multiple <code>vpn</code> options, specifying one VPN number in each option. You can specify a single VPN identifier (such as <code>vpn 1</code>) or a range of VPN identifiers (such as <code>vpn 1-10</code>).</td>
<td>Configuration &gt; Policies &gt; Centralized Policy &gt; Add Policy &gt; Create Groups of Interest &gt; VPN or Configuration &gt; Policies &gt; Custom Options &gt; Centralized Policy &gt; Lists &gt; VPN <code>vpn-list list-name</code> <code>vpn vpn-id</code></td>
</tr>
</tbody>
</table>
VPN Lists

Each centralized data policy is associated with a VPN list. You configure VPN lists with the `policy data-policy vpn-list` command. The list you specify must be one that you created with a VPN Group of Interest or List in the Cisco vManage policy configuration wizard or with the `policy lists vpn-list` command.

For centralized data policy, you can include any VPNs except for VPN 0 and VPN 512. VPN 0 is reserved for control traffic, so never carries any data traffic, and VPN 512 is reserved for out-of-band network management, so also never carries any data traffic. Note that while the CLI allows you to include these two VPNs in a data policy configuration, the policy is not applied to these two VPNs.

Policer Parameters

To configure policing parameters, create a policer that specifies the maximum bandwidth and burst rate for traffic on an interface, and how to handle traffic that exceeds these values.

In the Cisco vManage NMS, you configure policer parameters from:

- Configuration > Policies > Centralized Policy > Add Policy > Create Groups of Interest > Policer
- Configuration > Policies > Custom Options > Centralized Policy > Lists > Policer

In the CLI, you configure policer parameters as follows:

```
vSmart(config)# policy policer policer-name
vSmart(config-policer)# rate bps
vSmart(config-policer)# burst bytes
vSmart(config-policer)# exceed action
```

- `rate` is the maximum traffic rate. It can be a value from 0 through 264 – 1 bits per second.
- `burst` is the maximum traffic burst size. It can be a value from 15000 to 1000000 bytes.
- `exceed` is the action to take when the burst size or traffic rate is exceeded. `action` can be `drop` (the default) or `remark`. The `drop` action is equivalent to setting the packet loss priority (PLP) bit to low. The `remark` action sets the PLP bit to high. In centralised data policy, access lists, and application-aware routing policy, you can match the PLP with the `match plp` option.

Sequences

Each VPN list consists of sequences of match–action pairs. The sequences are numbered to set the order in which data traffic is analyzed by the match–action pairs in the policy.

In the Cisco vManage NMS, you configure sequences from:

- Configuration > Policies > Centralized Policy > Add Policy > Configure Traffic Rules > (Application-Aware Routing | Traffic Data | Cflowd) > Sequence Type
- Configuration > Policies > Custom Options > Centralized Policy > Traffic Policy > (Application-Aware Routing | Traffic Data | Cflowd) > Sequence Type

In the CLI, you configure sequences with the `policy data-policy vpn-list sequence` command. Each sequence can contain one match condition and one action condition.
**Match Parameters**

Centralized data policy can match IP prefixes and fields in the IP headers, as well as applications. You can also enable split DNS.

In the Cisco vManage NMS, you configure match parameters from:

- **Configuration > Policies > Centralized Policy > Add Policy > Configure Traffic Rules > (Application-Aware Routing | Traffic Data | Cflowd) > Sequence Type > Sequence Rule > Match**
- **Configuration > Policies > Custom Options > Centralized Policy > Traffic Policy > (Application-Aware Routing | Traffic Data | Cflowd) > Sequence Type > Sequence Rule > Match**

Each sequence in a policy can contain one match condition.

For data policy, you can match these parameters:

<table>
<thead>
<tr>
<th>Description</th>
<th>vManage Configuration/CLI Configuration Command</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Match all packets</td>
<td>Omit Match</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>Omit <code>match</code> command</td>
<td></td>
</tr>
<tr>
<td>Applications or application</td>
<td>Match Applications/Application Family List</td>
<td>Name of an application list or an <code>app-list</code> list</td>
</tr>
<tr>
<td>families</td>
<td><code>app-list list-name</code></td>
<td></td>
</tr>
<tr>
<td>Group of destination prefixes</td>
<td>Match Destination Data Prefix <code>destination-data-prefix-list list-name</code></td>
<td>Name of a data prefix list or a <code>data-prefix-list</code> list</td>
</tr>
<tr>
<td>Individual destination prefix</td>
<td>Match Destination Data Prefix <code>destination-ip prefix/length</code></td>
<td>IP prefix and prefix length</td>
</tr>
<tr>
<td>Destination port number</td>
<td>Match Destination Port <code>destination-port number</code></td>
<td>0 through 65535; specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-])</td>
</tr>
<tr>
<td>Enable split DNS, to resolve and</td>
<td>Match DNS Application List <code>dns-app-list list-name</code></td>
<td>Name of an <code>app-list</code> list. This list specifies the applications whose DNS requests are processed.</td>
</tr>
<tr>
<td>process DNS requests and</td>
<td></td>
<td></td>
</tr>
<tr>
<td>responses on an application-by-</td>
<td></td>
<td></td>
</tr>
<tr>
<td>application basis</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Specify the direction in which</td>
<td>Match DNS `dns (request</td>
<td>response)`</td>
</tr>
<tr>
<td>to process DNS packets</td>
<td></td>
<td>To process DNS requests sent by the applications (for outbound DNS queries), specify <code>dns request</code>. To process DNS responses returned from DNS servers to the applications, specify <code>dns response</code>.</td>
</tr>
</tbody>
</table>

**Policies Configuration Guide for vEdge Routers, Cisco SD-WAN Releases 19.1, 19.2, and 19.3**
### Action Parameters

When data traffic matches the conditions in the match portion of a centralized data policy, the packet can be accepted or dropped, and it can be counted. Then, you can associate parameters with accepted packets.

In the Cisco vManage NMS, you configure match parameters from:

- **Configuration > Policies > Centralized Policy > Add Policy > Configure Traffic Rules > (Application-Aware Routing | Traffic Data | Cflowd) > Sequence Type > Sequence Rule > Action**

- **Configuration > Policies > Custom Options > Centralized Policy > Traffic Policy > (Application-Aware Routing | Traffic Data | Cflowd) > Sequence Type > Sequence Rule > Action.**

In the CLI, you configure the action parameters with the `policy data-policy vpn-list sequence action` command.

Each sequence in a centralized data policy can contain one action condition.

In the action, you first specify whether to accept or drop a matching data packet, and whether to count it:

<table>
<thead>
<tr>
<th>Description</th>
<th>vManage Configuration/CLI Configuration Command</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSCP value</td>
<td>Match DSCP</td>
<td>0 through 63</td>
</tr>
<tr>
<td></td>
<td><code>dscp number</code></td>
<td></td>
</tr>
<tr>
<td>Packet length</td>
<td>Match Packet Length</td>
<td>0 through 65535; specify a single length, a list of lengths (with numbers separated by a space), or a range of lengths (with the two numbers separated with a hyphen [-])</td>
</tr>
<tr>
<td></td>
<td><code>packet-length number</code></td>
<td></td>
</tr>
<tr>
<td>Packet loss priority (PLP)</td>
<td>Match PLP</td>
<td>(high</td>
</tr>
<tr>
<td></td>
<td><code>plp</code></td>
<td></td>
</tr>
<tr>
<td>Internet protocol number</td>
<td>Match Protocol</td>
<td>0 through 255</td>
</tr>
<tr>
<td></td>
<td><code>protocol number</code></td>
<td></td>
</tr>
<tr>
<td>Group of source prefixes</td>
<td>Match Source Data Prefix</td>
<td>Name of a data prefix or a data-prefix-list list</td>
</tr>
<tr>
<td></td>
<td><code>source-data-prefix-list list-name</code></td>
<td></td>
</tr>
<tr>
<td>Individual source prefix</td>
<td>Match Source Data Prefix</td>
<td>IP prefix and prefix length</td>
</tr>
<tr>
<td></td>
<td><code>source-ip prefix/length</code></td>
<td></td>
</tr>
<tr>
<td>Source port number</td>
<td>Match Source Port</td>
<td>0 through 65535; specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-])</td>
</tr>
<tr>
<td></td>
<td><code>source-port address</code></td>
<td></td>
</tr>
<tr>
<td>TCP flag</td>
<td><code>tcp flag</code></td>
<td>syn</td>
</tr>
<tr>
<td>Description</td>
<td>vManage Configuration/CLI Configuration Parameter</td>
<td>Value or Range</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------</td>
<td>--------------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Accept the packet. An accepted packet is eligible to be modified by the additional parameters configured in the action portion of the policy configuration.</td>
<td>Click Accept, accept</td>
<td>—</td>
</tr>
<tr>
<td>Enable cflowd traffic monitoring.</td>
<td>Click Accept, then action Cflowd cflowd</td>
<td>—</td>
</tr>
<tr>
<td>Count the accepted or dropped packets.</td>
<td>Action Counter</td>
<td>Name of a counter. Use the <code>show policy access-lists counters</code> command on the Cisco device.</td>
</tr>
<tr>
<td>Discard the packet. This is the default action.</td>
<td>Click Drop drop</td>
<td>—</td>
</tr>
<tr>
<td>Log the packet. Packets are placed into the messages and vsyslog system logging (syslog) files.</td>
<td>Action Log</td>
<td>To view the packet logs, use the <code>show app log flows</code> and <code>show log</code> commands.</td>
</tr>
</tbody>
</table>
| Redirect DNS requests to a particular DNS server. Redirecting requests is optional, but if you do so, you must specify both actions. | Click Accept, then action Redirect DNS redirect-dns host redirect-dns ip-address | For an inbound policy, `redirect-dns host` allows the DNS response to be correctly forwarded back to the requesting service VPN.  
For an outbound policy, specify the IP address of the DNS server. |
| Fine-tune TCP to decrease round-trip latency and improve throughput for matching TCP traffic. | Click Accept, then action TCP Optimization tcp-optimization | —              |

Then, for a packet that is accepted, the following parameters can be configured:

<table>
<thead>
<tr>
<th>Description</th>
<th>vManage</th>
<th>CLI Configuration Parameter</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable cflowd traffic monitoring.</td>
<td>Click Accept, then action Cflowd cflowd</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>Direct matching traffic to the NAT functionality so that it can be redirected directly to the Internet or other external destination.</td>
<td>Click Accept, then action NAT Pool or NAT VPN. nat [pool number] [use-vpn 0]</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>vManage</td>
<td>CLI Configuration Parameter</td>
<td>Value or Range</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>--------------------------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>DSCP value.</td>
<td>Click <strong>Accept</strong>, then action <strong>DSCP</strong>.</td>
<td><strong>set dscp value</strong></td>
<td>0 through 63</td>
</tr>
<tr>
<td>Forwarding class.</td>
<td>Click <strong>Accept</strong>, then action <strong>Forwarding Class</strong>.</td>
<td><strong>set forwarding-class value</strong></td>
<td>Name of forwarding class</td>
</tr>
<tr>
<td>Direct matching packets to a TLOC that matches the color and encapsulation</td>
<td>Click <strong>Accept</strong>, then action <strong>Local TLOC</strong>.</td>
<td><strong>set local-tloc color [encap encapsulation]</strong></td>
<td>color can be:</td>
</tr>
<tr>
<td>By default, if the TLOC is not available, traffic is forwarded using an</td>
<td></td>
<td></td>
<td>3g, biz-internet,</td>
</tr>
<tr>
<td>alternate TLOC.</td>
<td></td>
<td></td>
<td>blue,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>bronze, custom1,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>custom2,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>custom3, default,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>gold,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>green, lte,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>metro-ethernet,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>mpls, private1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>through private6,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>public-internet, red,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>and silver.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>By default,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>encapsulation</strong> is ipsec.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>It can also be gre.</td>
</tr>
<tr>
<td>Direct matching packets to one of the TLOCs in the list if the TLOC</td>
<td>Click <strong>Accept</strong>, then action <strong>Local TLOC</strong>.</td>
<td><strong>set local-tloc-list color color encap</strong></td>
<td></td>
</tr>
<tr>
<td>matches the color and encapsulation</td>
<td></td>
<td><strong>encapsulation [restrict]</strong></td>
<td></td>
</tr>
<tr>
<td>By default, if the TLOC is not available, traffic is forwarded using an</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>alternate TLOC.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Set the next hop to which the packet should be forwarded.</td>
<td>Click <strong>Accept</strong>, then action <strong>Next Hop</strong>.</td>
<td><strong>set next-hop ip-address</strong></td>
<td>IP address</td>
</tr>
<tr>
<td>Apply a policer.</td>
<td>Click <strong>Accept</strong>, then action <strong>Policer</strong>.</td>
<td><strong>set policer policer-name</strong></td>
<td>Name of policer configured</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>with a <strong>policy policer</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>command.</td>
</tr>
</tbody>
</table>
Specify a service to redirect traffic to before delivering the traffic to its destination.

The TLOC address or list of TLOCs identifies the remote TLOCs to which the traffic should be redirected to reach the service. In the case of multiple TLOCs, the traffic is load-balanced among them.

The VPN identifier is where the service is located.

Configure the services themselves on the Cisco devices that are collocated with the service devices, using the `vpn service` command.

Direct traffic to a remote TLOC that matches the IP address, color, and encapsulation.

Direct traffic to one of the remote TLOCs in the TLOC list if it matches the IP address, color, and encapsulation of one of the TLOCs in the list. If a preference value is configured for the matching TLOC, that value is assigned to the traffic.

Set the VPN that the packet is part of.

The following table describes the IPv4 and IPv6 actions.

<table>
<thead>
<tr>
<th>IPv4 Actions</th>
<th>IPv6 Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>drop, dscp, next-hop (from-service only)/vpn, count, forwarding class, policer (only in interface ACL), App-route SLA (only)</td>
<td>drop, dscp, next-hop/vpn, count, forwarding class, policer (only in interface ACL)</td>
</tr>
<tr>
<td>App-route preferred color, app-route sla strict, cflowd, nat, redirect-dns</td>
<td>App-route SLA (only), App-route preferred color, app-route sla strict</td>
</tr>
<tr>
<td>policer (DataPolicy), tcp-optimization, fec-always,</td>
<td>policer (DataPolicy)</td>
</tr>
</tbody>
</table>
Default Action

If a data packet being evaluated does not match any of the match conditions in a data policy, a default action is applied to the packet. By default, the data packet is dropped.

In the Cisco vManage NMS, you modify the default action from:


In the CLI, you modify the default action with the `policy data-policy vpn-list default-action accept` command.

Apply Centralized Data Policy

For a centralized data policy to take effect, you apply it to a list of sites in the overlay network.

To apply a centralized policy in the Cisco vManage NMS:

1. In the Cisco vManage NMS, select the Configure > Policies screen.
2. Select a policy from the policy table.
3. Click the More Actions icon to the right of the row, and click Activate. The Activate Policy popup opens. It lists the IP addresses of the reachable Cisco vSmart Controllers to which the policy is to be applied.
4. Click Activate.

To apply a centralized policy in the CLI:

`vSmart(config)# apply-policy site-list list-name data-policy policy-name (all | from-service | from-tunnel)`

By default, data policy applies to all data traffic passing through the Cisco device: the policy evaluates all data traffic going from the local site (that is, from the service side of the router) into the tunnel interface, and it evaluates all traffic entering to the local site through the tunnel interface. You can explicitly configure this behavior by including the all option. To have the data policy apply only to traffic coming from the service site and exiting from the local site through the tunnel interface, include the from-service option. To have the policy apply only to traffic entering from the tunnel interface and traveling to the service site, include the from-tunnel option. You can apply different data policies in each of the two traffic directions.

For all data-policy policies that you apply with apply-policy commands, the site IDs across all the site lists must be unique. That is, the site lists must not contain overlapping site IDs. An example of overlapping site IDs are those in the two site lists site-list 1 site-id 1-100 and site-list 2 site-id 70-130. Here, sites 70 through
100 are in both lists. If you were to apply these two site lists to two different `data-policy` policies, the attempt to commit the configuration on the Cisco vSmart Controller would fail.

The same type of restriction also applies to the following types of policies:

- Application-aware routing policy (`app-route-policy`)
- Centralized control policy (`control-policy`)
- Centralized data policy used for cflowd flow monitoring (`data-policy` that includes a `cflowd` action and `apply-policy` that includes a `cflowd-template` command)

You can, however, have overlapping site IDs for site lists that you apply for different types of policy. For example, the sites lists for `control-policy` and `data-policy` policies can have overlapping site IDs. So for the two example site lists above, `site-list 1 site-id 1-100` and `site-list 2 site-id 70-130`, you could apply one to a control policy and the other to a data policy.

As soon as you successfully activate the configuration by issuing a `commit` command, the Cisco vSmart Controller pushes the data policy to the devices located in the specified sites. To view the policy as configured on the Cisco vSmart Controllers, use the `show running-config` command on the Cisco vSmart Controller:

```
vSmart# show running-config policy
vSmart# show running-config apply-policy
```

To view the policy that has been pushed to the Cisco vEdge device, use the `show policy from-vsmart` command on the Cisco vEdge device.

```
vEdge# show policy from-vsmart
```

## Deep Packet Inspection

You configure deep packet inspection using a standard centralized data policy. You define the applications of interest in a vManage policy list or with `policy lists app-list` CLI command, and you call these lists in the match portion of the data policy. You can control the path of the application traffic through the network by defining, in the `action` portion of the data policy, the local TLOC or the remote TLOC, or for strict control, you can define both.

### Configure Deep Packet Inspection Using vManage

To configure a centralized data policy for deep packet inspection, use the vManage policy configuration wizard. Use the wizard to create and edit deep packet inspection policy components:

- Configure groups of interest (lists) to group related items to be called in the centralized data policy.
- Configure traffic rules.
- Apply the policy.

#### Step 1: Start the Policy Configuration Wizard

To start the policy configuration wizard:

1. In vManage NMS, select the Configure > Policies screen.
2. Select the Centralized Policy tab.
3. Click Add Policy.
The policy configuration wizard opens, and the Create Groups of Interest screen is displayed.

**Step 2: Create Groups of Interest**

In Create Groups of Interest, create lists of groups to use in centralized policy:

To configure groups of interest for deep packet inspection:

1. In the left pane, select the type of list. For centralized data policy for deep packet inspection, you can use Application, Site, and VPN lists.

2. To create a new list, click New List.
   
   To modify an existing list, click the More Actions icon to the right of the desired list, and click the pencil icon.

3. In the List Name field, enter a name for the list. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.

4. In the field below the List Name field, enter the desired values for the list. For some lists you type the desired values, and for others you select from a drop-down.

5. Click Add (for a new list) or Save (for an existing list).

6. Click Next to move to the Configure Topology and VPN Membership screen.

7. Click Next to move the Configure Traffic Rules in the wizard.

**Step 3: Configure Traffic Rules**

When you first open the Traffic Rules screen, the Application-Aware Routing tab is selected by default:

To configure traffic rules for deep packet inspection policy:

1. In the Application-Aware Routing bar, click Traffic Data.

2. To create a new centralized data policy, click Add Policy.
   
   To modify an existing policy, click the More Actions icon to the right of the desired policy, and click the pencil icon.

3. If data traffic does not match any of the conditions in one of the sequences, it is dropped by default. If you want nonmatching routes to be accepted, click the pencil icon in the Default Action, click Accept, and click Save Match And Actions.

4. To create a match–action sequence for data traffic:
   
   a. Click Sequence Type.

   b. To create a match–action rule, click Sequence Rule. The Match button is selected by default.

   c. Click the desired Match button, and enter the desired values in Match Conditions. For some conditions, you type the desired values, and for others you select from a drop-down.

   d. Click the Actions button. The default action is Reject. To accept matching packets, click the Accept radio button. Then click the desired action, and enter the desired values for Actions.

   e. Click Save Match and Actions.
f. Create additional Sequence Rules or Sequence Types, as needed.

5. To rename a Sequence Type, double-click its name in the right pane, and type the new name. The name also changes in the right pane.

6. To re-order sequence rules and types, drag and drop them them.

7. Click Save.

8. Click Next to move to the Apply Policies to Sites and VPNs in the wizard.

Step 4: Apply Policies to Sites and VPNs

1. In Apply Policies to Sites and VPNs, apply a policy to overlay network sites and VPNs:

2. In the Policy Name field, enter a name for the policy. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores (_). It cannot contain spaces or any other characters.

3. In the Policy Description field, enter a description of the policy. It can contain up to 2048 characters. This field is mandatory, and it can contain any characters and spaces.

4. From the Topology bar, select the Application-Aware Routing tab. The table then lists policies that you have created for that type of policy block.

5. Click Add New Site List and VPN List or Add New Site. Some topology blocks might have no Add buttons. Select one or more site lists, and select one or more VPN lists. Click Add.

6. Click Preview to view the configured policy. The policy is displayed in CLI format.

7. Click Save Policy. The Configuration > Policies screen opens, and the policies table includes the newly created policy.

Step 5: Activate a Centralized Data Policy

Activating a centralized data policy sends that policy to all connected vSmart controllers. To activate a centralized policy:

1. In vManage NMS, select the Configure > Policies screen.

2. Select a policy from the policy table.

3. Click the More Actions icon to the right of the row, and click Activate. The Activate Policy popup opens. It lists the IP addresses of the reachable vSmart controllers to which the policy is to be applied.

4. Click Activate.

Configure Deep Packet Inspection Using CLI

Following are the high-level steps for configuring a centralized data policy to use for deep packet inspection:

1. Create a list of overlay network sites to which the data policy is to be applied in the apply-policy command:

```
vSmart(config)# policy
vSmart(config-policy)# lists site-list list-name
vSmart(config-lists-list-name)# site-id site-id
```
The list can contain as many site IDs as necessary. Include one `site-id` command for each site ID. For contiguous site IDs, you can specify a range of numbers separated with a dash (–).

Create additional site lists, as needed.

2. Create lists of applications and application families that are to be subject to the data policy. Each list can contain one or more application names, or one or more application families. A single list cannot contain both applications and application families.

```plaintext
vSmart(config)# policy lists
vSmart(config-lists)# app-list list-name
vSmart(config-app-list)# app application-name
```

```plaintext
vSmart(config)# policy lists
vSmart(config-lists)# app-list list-name
vSmart(config-applist)# app-family family-name
```

3. Create lists of IP prefixes and VPNs, as needed:

```plaintext
vSmart(config)# policy lists
vSmart(config-lists)# data-prefix-list list-name
vSmart(config-lists-list-name)# ip-prefix prefix/length
```

```plaintext
vSmart(config)# policy lists
vSmart(config-lists)# vpn-list list-name
vSmart(config-lists-list-name)# vpn vpn-id
```

4. Create lists of TLOCs, as needed:

```plaintext
vSmart(config)# policy
vSmart(config-policy)# lists tloc-list list-name
vSmart(config-lists-list-name)# tloc ip-address color color encap encapsulation [preference number]
```

5. Define policing parameters, as needed:

```plaintext
vSmart(config-policy)# policer policer-name
vSmart(config-policer)# rate bandwidth
vSmart(config-policer)# burst bytes
vSmart(config-policer)# exceed action
```

6. Create a data policy instance and associate it with a list of VPNs:

```plaintext
vSmart(config)# policy data-policy policy-name
vSmart(config-data-policy-policy-name)# vpn-list list-name
```

7. Create a series of match–action sequences:

```plaintext
vSmart(config-vpn-list)# sequence number
vSmart(config-sequence-number)#
```

The match–action pairs are evaluated in order, by sequence number, starting with the lowest numbered pair and ending when the route matches the conditions in one of the pairs. Or if no match occurs, the default action is taken (either rejecting the route or accepting it as is).

8. Define match parameters based on applications:

```plaintext
vSmart(config-sequence-number)# match app-list list-name
```

9. Define additional match parameters for data packets:

```plaintext
vSmart(config-sequence-number)# match parameters
```

10. Define actions to take when a match occurs:

```plaintext
vSmart(config-sequence-number)# action (accept | drop) [count]
```
11. For packets that are accepted, define the actions to take. To control the tunnel over which the packets travels, define the remote or local TLOC, or for strict control over the tunnel path, set both:

   vSmart(config-action)# set tloc ip-address color color encap encapsulation
   vSmart(config-action)# set tloc-list list-name
   vSmart(config-action)# set local-tloc-list color color encap encapsulation [restrict]

12. Define additional actions to take.

13. Create additional numbered sequences of match–action pairs within the data policy, as needed.

14. If a route does not match any of the conditions in one of the sequences, it is rejected by default. If you want nonmatching prefixes to be accepted, configure the default action for the policy:

   vSmart(config-policy-name)# default-action accept

15. Apply the policy to one or more sites in the overlay network:

   vSmart(config)# apply-policy site-list list-name data-policy policy-name (all | from-service | from-tunnel)

   To enable the infrastructure for deep packet inspection on the vEdge routers, include the following command in the configuration on the routers:

   vEdge(config)# policy app-visibility

### Structural Components of Policy Configuration for Deep Packet Inspection

Following are the structural components required to configure centralized data policy for deep packet inspection. Each one is explained in more detail in the sections below.

On the vSmart controller:

- **policy**
- **lists**
  - **app-list** list-name
    - (app applications | app-family application-families)
  - **data-prefix-list** list-name
  - **ip-prefix** prefix
  - **site-list** list-name
  - **site-id** site-id
  - **tloc-list** list-name
  - **tloc** ip-address color color encap encapsulation [preference value]
  - **vpn-list** list-name
  - **vpn** vpn-id
  - **policer** policer-name
  - **burst** bytes
  - **exceed** action
  - **rate** bps
- **data-policy** policy-name
- **vpn-list** list-name
- **sequence** number
- **match**
  - **app-list** list-name
  - **destination-data-prefix-list** list-name
  - **destination-ip** ip-addresses
  - **destination-port** port-numbers
  - **dscp** number
  - **packet-length** number
  - **protocol** protocol
  - **source-data-prefix-list** list-name
  - **source-ip** ip-addresses
  - **source-port** port-numbers
  - **tcp** flag
- **action**
drop
count counter-name
log
accept
nat [pool number] [use-vpn 0]
set
dscp number
forwarding-class class
local-tloc color color [encap encapsulation] [restrict]
next-hop ip-address
policer policer-name
service service-name local [restrict] [vpn vpn-id]
service-service-name (tloc ip-address | tloc-list list-name) [vpn vpn-id]
tloc ip-address color color encap encapsulation
tloc-list list-name
vpn vpn-id
default-action
(accept | drop)
apply-policy site-list list-name
data-policy policy-name (all | from-service | from-tunnel)

On the vEdge router:
policy
app-visibility

Action Parameters for Configuring Deep Packet Inspection

When data traffic matches the conditions in the match portion of a centralized data policy, the packet can be accepted or dropped, and it can be counted. Then, you can associate parameters with accepted packets.

In vManage NMS, you configure match parameters from:

- Configuration > Policies > Centralized Policy > Add Policy > Configure Traffic Rules > (Application-Aware Routing | Traffic Data | Cflowd) > Sequence Type > Sequence Rule > Action

In the CLI, you configure the action parameters under the **policy data-policy vpn-list sequence action** command.

Each sequence in a centralized data policy can contain one action condition.

In the action, you first specify whether to accept or drop a matching data packet, and whether to count it:

<table>
<thead>
<tr>
<th>Description</th>
<th>vManage Configuration/CLI Configuration Parameter</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept the packet. An accepted packet is eligible to be modified by the additional parameters configured in the action portion of the policy configuration.</td>
<td>Click Accept. accept</td>
<td>—</td>
</tr>
<tr>
<td>Count the accepted or dropped packets.</td>
<td>Action Counter</td>
<td>Name of a counter. Use the <strong>show policy access-lists counters</strong> command on the Cisco device.</td>
</tr>
</tbody>
</table>
### Action Parameters for Configuring Deep Packet Inspection

<table>
<thead>
<tr>
<th>Description</th>
<th>vManage Configuration/CLI Configuration Parameter</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discard the packet. This is the default action.</td>
<td>Click <strong>Drop</strong> drop</td>
<td>—</td>
</tr>
<tr>
<td>Log the packet. Packets are placed into the messages and vsyslog system logging (syslog) files.</td>
<td>Action Log Click <strong>Accept</strong>, then action <strong>Log</strong> log</td>
<td>To view the packet logs, use the <code>show app log flows</code> and <code>show log</code> commands.</td>
</tr>
</tbody>
</table>

To view the packet logs, use the `show app log flows` and `show log` commands.

Then, for a packet that is accepted, the following parameters can be configured. Note that you cannot use DPI with either cflowd or NAT.

<table>
<thead>
<tr>
<th>Description</th>
<th>vManage</th>
<th>CLI Configuration Parameter</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSCP value.</td>
<td>Click <strong>Accept</strong>, then action <strong>DSCP</strong>.</td>
<td>set <strong>dscp</strong> value</td>
<td>0 through 63</td>
</tr>
<tr>
<td>Forwarding class.</td>
<td>Click <strong>Accept</strong>, then action <strong>Forwarding Class</strong>.</td>
<td>set <strong>forwarding-class</strong> value</td>
<td>Name of forwarding class</td>
</tr>
<tr>
<td>Direct matching packets to a TLOC that matches the color and encapsulation By default, if the TLOC is not available, traffic is forwarded using an alternate TLOC.</td>
<td>Click <strong>Accept</strong>, then action <strong>Local TLOC</strong>.</td>
<td>set local-tloc color [encap encapsulation]</td>
<td>color can be: 3g, biz-internet, blue, bronze, custom1, custom2, custom3, default, gold, green lte, metro-ethernet, mpls, private1 through private6, public-internet, red, and silver. By default, encapsulation is ipsec. It can also be gre.</td>
</tr>
<tr>
<td>Direct matching packets to one of the TLOCs in the list if the TLOC matches the color and encapsulation By default, if the TLOC is not available, traffic is forwarded using an alternate TLOC. To drop traffic if a TLOC is unavailable, include the <strong>restrict</strong> option.</td>
<td>Click <strong>Accept</strong>, then action <strong>Local TLOC</strong></td>
<td>set local-tloc-list color color encap encapsulation [restrict]</td>
<td></td>
</tr>
<tr>
<td>Set the next hop to which the packet should be forwarded.</td>
<td>Click <strong>Accept</strong>, then action <strong>Next Hop</strong>.</td>
<td>set next-hop <strong>ip-address</strong></td>
<td>IP address</td>
</tr>
<tr>
<td>Apply a policer.</td>
<td>Click <strong>Accept</strong>, then action <strong>Policer</strong>.</td>
<td>set <strong>policer</strong> <strong>policer-name</strong></td>
<td>Name of policer configured with a <strong>policy policer</strong> command.</td>
</tr>
</tbody>
</table>
### Description

<table>
<thead>
<tr>
<th>Value or Range</th>
<th>CLI Configuration Parameter</th>
<th>vManage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard services: FW, IDS, IDP</td>
<td>`set service service-name [tloc ip-address</td>
<td>tloc-list list-name] [vpn vpn-id]`</td>
</tr>
<tr>
<td>Custom services: netsvc1, netsvc2, netsvc3, netsvc4</td>
<td>TLOC list is configured with a <code>policy lists tloc-list</code> list.</td>
<td></td>
</tr>
<tr>
<td>TLOC address, color, and encapsulation</td>
<td><code>set local-tloc color [encap encapsulation]</code></td>
<td>Click Accept, then action TLOC.</td>
</tr>
<tr>
<td>Name of a <code>policy lists tloc-list</code> list</td>
<td><code>set tloc-list list-name</code></td>
<td>Click Accept, then action TLOC.</td>
</tr>
<tr>
<td>Set the VPN that the packet is part of.</td>
<td><code>set vpn vpn-id</code></td>
<td>Click Accept, then action VPN.</td>
</tr>
</tbody>
</table>

#### Default Action

If a data packet being evaluated does not match any of the match conditions in a data policy, a default action is applied to the packet. By default, the data packet is dropped.

In vManage NMS, you modify the default action from `Configuration > Policies > Centralized Policy > Add Policy > Configure Traffic Rules > Application-Aware Routing > Sequence Type > Sequence Rule > Default Action`.  

---

<table>
<thead>
<tr>
<th>Description</th>
<th>CLI Configuration Parameter</th>
<th>vManage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct matching packets to the named service that is reachable via a GRE tunnel whose source is in the transport VPN (VPN 0). If the GRE tunnel used to reach the service is down, packet routing falls back to using standard routing. To drop packets when a GRE tunnel to the service is unreachable, include the restrict option. In the service VPN, you must also advertise the service using the <code>service</code> command. You configure the GRE interface or interfaces in the transport VPN (VPN 0).</td>
<td>`set service service-name [tloc ip-address</td>
<td>tloc-list list-name] [vpn vpn-id]`</td>
</tr>
<tr>
<td>Direct traffic to a remote TLOC. The TLOC is defined by its IP address, color, and encapsulation.</td>
<td><code>set local-tloc color [encap encapsulation]</code></td>
<td>Click Accept, then action TLOC.</td>
</tr>
<tr>
<td>Direct traffic to one of the remote TLOCs in the TLOC list.</td>
<td><code>set tloc-list list-name</code></td>
<td>Click Accept, then action TLOC.</td>
</tr>
<tr>
<td>Set the VPN that the packet is part of.</td>
<td><code>set vpn vpn-id</code></td>
<td>Click Accept, then action VPN.</td>
</tr>
</tbody>
</table>
In the CLI, you modify the default action with the `policy data-policy vpn-list default-action accept` command.

### Apply Centralized Data Policy for Deep Packet Inspection

For a deep packet inspection centralized data policy to take effect, you apply it to a list of sites in the overlay network.

To apply a centralized policy in vManage NMS:

1. In vManage NMS, select the Configure > Policies screen.
2. Select a policy from the policy table.
3. Click the More Actions icon to the right of the row, and click Activate. The Activate Policy popup opens. It lists the IP addresses of the reachable vSmart controllers to which the policy is to be applied.
4. Click Activate.

To apply a centralized policy in the CLI:

```
vSmart(config)# apply-policy site-list list-name data-policy policy-name (all | from-service | from-tunnel)
```

By default, data policy applies to all data traffic passing through the vEdge router: the policy evaluates all data traffic going from the local site (that is, from the service side of the router) into the tunnel interface, and it evaluates all traffic entering to the local site through the tunnel interface. You can explicitly configure this behavior by including the `all` option. To have the data policy apply only to policy exiting from the local site, include the `from-service` option. To have the policy apply only to incoming traffic, include the `from-tunnel` option.

You cannot apply the same type of policy to site lists that contain overlapping site IDs. That is, all data policies cannot have overlapping site lists among themselves. If you accidentally misconfigure overlapping site lists, the attempt to commit the configuration on the vSmart controller fails.

As soon as you successfully activate the configuration by issuing a `commit` command, the vSmart controller pushes the data policy to the vEdge routers located in the specified sites. To view the policy as configured on the vSmart controller, use the `show running-config policy` command on the vSmart controller:

```
vSmart# show running-config policy
vSmart# ;show running-config apply-policy
```

To view the policy that has been pushed to the vEdge router, use the `show policy from-vsmart` command on the vEdge router.

```
vEdge# show policy from-vsmart
```

### Monitor Running Applications

To enable the deep packet inspection infrastructure on the vEdge routers, you must enable application visibility on the routers:

```
vEdge(config)# policy app-visibility
```

To display information about the running applications, use the `show app dpi supported-applications`, `show app dpi applications`, and `show app dpi flows` commands on the router.
View DPI Applications Using vManage

You can view the list of all the application-aware applications supported by the SD-WAN software on the router using the following steps:

1. In the Cisco vManage, select the Monitor > Network screen.
2. From the WAN-Edge pane, select the Device that supports DPI. The vManage Control Connections page displays.
3. In the left pane, select Real Time to view the device details.
4. From the Device Options drop-down, choose DPI Applications to view the list of applications running on the device.
5. From the Device Options drop-down, choose DPI Supported Applications to view the list of applications that are supported on the device.

Configure VPN Membership Policy

A VPN membership data policy consists of a series of numbered (ordered) sequences of match-action pair that are evaluated in order, from lowest sequence number to highest sequence number. When a packet matches one of the match conditions, the associated action is taken and policy evaluation on that packets stops. Keep this in mind as you design your policies to ensure that the desired actions are taken on the items subject to policy.

If a packet matches no parameters in any of the sequences in the policy configure, it is, by default, rejected and discarded.

To create a VPN membership policy, you include the following components in the configuration on a vSmart controller:

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>vManage Configuration</th>
<th>CLI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lists</td>
<td>Groupings of related items that you reference in the match and action portions of the data policy configuration. For VPN membership policy, you can group sites and VPNs.</td>
<td>Configuration &gt; Policies &gt; Centralized Policy &gt; Add Policy &gt; Create Groups of Interest or Configuration &gt; Policies &gt; Custom Options &gt; Centralized Policy &gt; Lists</td>
<td>policy lists</td>
</tr>
<tr>
<td>Centralized VPN membership policy instance</td>
<td>Container for VPN membership policy to filter packets based on VPN.</td>
<td>Configuration &gt; Policies &gt; Centralized Policy &gt; Add Policy</td>
<td>policy vpn-membership</td>
</tr>
<tr>
<td>Component</td>
<td>Description</td>
<td>vManage Configuration</td>
<td>CLI</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>VPN membership</td>
<td>Conditions that define the VPN members.</td>
<td>Configuration &gt; Policies &gt; Centralized Policy &gt; Add Policy &gt; Configure Topology and VPN Membership &gt; Add VPN Membership Policy or Configuration &gt; Policies &gt; Custom Options &gt; Centralized Policy &gt; Topology &gt; Add VPN Membership Policy</td>
<td>—</td>
</tr>
</tbody>
</table>
| Numbered sequences of            | Sequences that establish the order in which the policy components are        | Configuration > Policies > Centralized Policy > Add Policy > Configure Traffic Rules > Traffic Data > Sequence Type or Configuration > Policies > Custom Options > Centralized Policy > Traffic Policy > Traffic Data > Sequence Type | policy data-policy  
vpn-list sequence |
| match–action pairs               | applied.                                                                     |                                                                                                                                                                         |                                                                      |
| Match parameters                 | Conditions that packets must match to be considered for the VPN membership  | Configuration > Policies > Centralized Policy > Add Policy > Configure Traffic Rules > Traffic Data > Sequence Type > Sequence Rule or Configuration > Policies > Custom Options > Centralized Policy > Traffic Policy > Traffic Data > Sequence Type > Sequence Rule | policy vpn-membership  
sequence match |
|                                 | policy                                                                      |                                                                                                                                                                         |                                                                      |
Centralized Data Policy Configuration Examples

This topic provides some straightforward examples of configuring centralized data policy to influence traffic flow across the Cisco SD-WAN domain and to configure a Cisco device to be an Internet exit point.

**General Centralized Data Policy Example**

This section shows a general example of a centralized data policy to illustrate that you configure centralized data policy on a Cisco vSmart Controller and that after you commit the configuration, the policy itself is pushed to the required Cisco devices.

Here we configure a simple data policy on the Cisco vSmart Controller vm9:

---

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>vManage Configuration</th>
<th>CLI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actions</td>
<td>Whether to accept or reject matching packets.</td>
<td>Configuration &gt; Policies &gt; Centralized Policy &gt; Add Policy &gt; Configure Traffic Rules &gt; Traffic Data &gt; Sequence Type &gt; Sequence Rule or Configuration &gt; Policies &gt; Custom Options &gt; Centralized Policy &gt; Traffic Policy &gt; Traffic Data &gt; Sequence Type &gt; Sequence Rule</td>
<td><code>policy vpn-membership sequence action</code></td>
</tr>
<tr>
<td>Default action</td>
<td>Action to take if a packet matches none of the policy conditions.</td>
<td>Configuration &gt; Policies &gt; Centralized Policy &gt; Add Policy &gt; Configure Traffic Rules &gt; Traffic Data &gt; Sequence Type &gt; Default Action or Configuration &gt; Policies &gt; Custom Options &gt; Centralized Policy &gt; Traffic Policy &gt; Traffic Data &gt; Sequence Type &gt; Default Action</td>
<td><code>policy vpn-membership default-action</code></td>
</tr>
<tr>
<td>Application of VPN membership policy</td>
<td>For a VPN membership policy to take effect, you apply it to one or more sites in the overlay network.</td>
<td>Configuration &gt; Policies &gt; Centralized Policy &gt; Add Policy &gt; Apply Policies to Sites and VPNs</td>
<td><code>apply-policy site-list vpn-membership</code></td>
</tr>
</tbody>
</table>
Immediately after we activate the configuration on the Cisco vSmart Controller, it pushes the policy configuration to the Cisco vEdge devices in site 500. One of these devices is vm5, where we see that the policy has been received:

```
vm5# show policy from-vsmart
policy-from-vsmart
data-policy test-data-policy
vpn-list test-vpn-list
   sequence 10
   match
      destination-ip 209.165.201.0/27
      action drop
      count test-counter
      !
      default-action drop
      !
      !
lists
vpn-list test-vpn-list
   vpn 1
   !
site-list test-site-list
   site-id 500
   !
   !
```

**Control Access**

This example shows a data policy that limits the type of packets that a source can send to a specific destination. Here, the host at source address 192.0.2.1 in site 100 and VPN 100 can send only TCP traffic to the destination host at 203.0.113.1. This policy also specifies the next hop for the TCP traffic sent by 192.0.2.1, setting it to be TLOC 209.165.200.225, color gold. All other traffic is accepted as a result of the `default-action` statement.

```
policy
lists
   site-list north
      site-id 100
```

Data Policies

Restrict Traffic

This example illustrates how to disallow certain types of data traffic from being sent from between VPNs. This policy drops data traffic on port 25, which carries SMTP mail traffic, that originates in 209.165.201.0/27. However, the policy accepts all other data traffic, including non-SMTP traffic from 209.165.201.0/27.

Allow Traffic to Exit from a Cisco vEdge Device to the Internet

The following example allows data traffic destined for two prefixes on the Internet to exit directly from the local Cisco vEdge device to the Internet destination. Configure this policy on the Cisco vSmart Controller.
Using the destination port instead of a destination IP prefix allows greater flexibility for traffic exiting to the Internet. Here, traffic can go to all HTTP and HTTPS sites (ports 80 and 443, respectively). Configure this policy on a Cisco vSmart Controller.

```plaintext
apply-policy
  site-list nat-sites data-policy accept-nat
```

**Localized Data Policy**

Data policy operates on the data plane in the Cisco SD-WAN overlay network and affects how data traffic is sent among the Cisco devices in the network. The Cisco SD-WAN architecture defines two types of data
policy, centralized data policy, which controls the flow of data traffic based on the IP header fields in the data packets and based on network segmentation, and localized data policy, which controls the flow of data traffic into and out of interfaces and interface queues on a Cisco device.

Localized data policy, so called because it is provisioned on the local Cisco device, is applied on a specific router interface and affects how a specific interface handles the data traffic that it is transmitting and receiving. Localized data policy is also referred to as access lists (ACLs). With access lists, you can provision class of service (CoS), classifying data packets and prioritizing the transmission properties for different classes. You can also provision packet mirroring and policing. For IPv4, you can also configure QoS actions.

You can apply IPv4 access lists in any VPN on the router, and you can create access lists that act on unicast and multicast traffic. You can apply IPv6 access lists only to tunnel interfaces in the transport VPN (VPN 0).

You can apply access lists either in the outbound or inbound direction on the interface. Applying an IPv4 ACL in the outbound direction affects data packets traveling from the local service-side network into the IPsec tunnel toward the remote service-side network. Applying an IPv4 ACL in the inbound direction affects data packets exiting from the IPsec tunnel and being received by the local Cisco device. For IPv6, an outbound ACL is applied to traffic being transmitted by the router, and an inbound ACL is applied to received traffic.

**Explicit and Implicit Access Lists**

Access lists that you configure using localized data policy are called *explicit* ACLs. You can apply explicit ACLs in any VPN on the device.

Router tunnel interfaces also have *implicit* ACLs, which are also referred to as *services*. Some of these are present by default on the tunnel interface, and they are in effect unless you disable them. Through configuration, you can also enable other implicit ACLs. On Cisco devices, the following services are enabled by default: DHCP (for DHCPv4 and DHCPv6), DNS, and ICMP. You can also enable services for BGP, Netconf, NTP, OSPF, SSHD, and STUN.

**Perform QoS Actions**

With access lists, you can provision quality of service (QoS) which allows you to classify data traffic by importance, spread it across different interface queues, and control the rate at which different classes of traffic are transmitted. See Forwarding and QoS Overview.

**Mirror Data Packets**

Once packets are classified, you can configure access lists to send a copy of data packets seen on a Cisco device interface to a specified destination on another network device. The Cisco SD-WAN software supports 1:1 mirroring; that is, a copy of every packet is sent to the alternate destination.

**Localized Data Policy for IPv4**

This topic provides procedures for configuring IPv4 localized data policy. This type of data policy is called access lists, or ACLs. You can provision simple access lists that filter traffic based on IP header fields. You also use access lists to apply QoS and policing to data packets. You can use access lists to apply mirroring on Cisco vEdge devices. You can create access lists that act on unicast and multicast traffic.

In the Cisco vManage NMS, you configure the localized data policy from the Configuration > Policies screen, using a policy configuration wizard. In the CLI, you configure these policies on the Cisco device.
**Configuration Components**

An access list consists of a sequences of match–action pairs that are evaluated in order, from lowest sequence number to highest sequence number. When a packet matches one of the match conditions, the associated action is taken and policy evaluation on that packets stops. Keep this in mind as you design your policies to ensure that the desired actions are taken on the items subject to policy.

If a packet matches no parameters in any of the sequences in the policy configuration, it is, by default, dropped.

The following figure illustrates the configuration components for access lists.

---

**Configure Localized Data Policy for IPv4 Using Cisco vManage**

To configure IPv4 localized policy, use the Cisco vManage policy configuration wizard. The wizard is a UI policy builder that consists of five screens to configure IPv4 localized policy components:

- **Groups of Interest**, also called lists—Create data prefix lists, mirroring, and policer parameters that group together related items and that you call in the match or action components of a policy.
- **Forwarding Classes**—Define forwarding classes and rewrite rules to use for QoS.
- **Access Control Lists**—Define the match and action conditions of ACLs.
- **Route Policies**—Define the match and action conditions of route policies.
- **Policy Settings**—Define additional policy settings, including Cloud QoS settings and the frequency for logging policy-related packet headers.

You configure some or all these components depending on the specific policy you are creating. To skip a component, click the **Next** button at the bottom of the screen. To return to a component, click the **Back** button at the bottom of the screen.

**Step 1: Start the Policy Configuration Wizard**

To start the policy configuration wizard:

1. In the Cisco vManage NMS, select the **Configure > Policies** screen.
2. Select the **Localized Policy** tab.
3. Click **Add Policy**.
The policy configuration wizard opens, and the Create Groups of Interest screen is displayed.

**Step 2: Create Groups of Interest**

In the Create Groups of interest screen create lists to use in the localized data policy:

1. Create news lists of groups, as described in the following table:

**Table 14:**

<table>
<thead>
<tr>
<th>List Type</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Prefix</td>
<td>1. In the left bar, click Data Prefix.</td>
</tr>
<tr>
<td></td>
<td>2. Click New Data Prefix List.</td>
</tr>
<tr>
<td></td>
<td>3. Enter a name for the list.</td>
</tr>
<tr>
<td></td>
<td>4. Enter one or more IP prefixes.</td>
</tr>
<tr>
<td></td>
<td>5. Click Add.</td>
</tr>
<tr>
<td>Mirror</td>
<td>1. In the left bar, click Mirror.</td>
</tr>
<tr>
<td></td>
<td>2. Click New Mirror List. The Mirror List popup displays.</td>
</tr>
<tr>
<td></td>
<td>3. Enter a name for the list.</td>
</tr>
<tr>
<td></td>
<td>4. In the Remote Destination IP field, enter the IP address of the destination to which to mirror the packets.</td>
</tr>
<tr>
<td></td>
<td>5. In the Source IP field, enter the IP address of the source of the packets to mirror.</td>
</tr>
<tr>
<td></td>
<td>6. Click Save.</td>
</tr>
<tr>
<td>List Type</td>
<td>Procedure</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------</td>
</tr>
</tbody>
</table>
| Policer   | 1. In the left bar, click **Policer**.  
|           | 2. Click **New Policer List**.  
|           | 3. Enter a name for the list.  
|           | 4. In the Burst field, enter maximum traffic burst size. It can be a value from 15000 to 10000000 bytes.  
|           | 5. In the Exceed field, select the action to take when the burst size or traffic rate is exceeded. Select **Drop** (the default) to set the packet loss priority (PLP) to low. Select **Remark** to set the PLP to high.  
|           | 6. In the Rate field, enter the maximum traffic rate. It can be value from 0 through $2^{64} - 1$ bps  
|           | 7. Click **Add**. |

1. Click **Next** to move to Configure Forwarding Classes/QoS in the wizard.

**Step 3: Configure Forwarding Classes for QoS**

When you first open the Forwarding Classes/QoS screen, the **QoS** tab is selected by default:

To configure forwarding classes for use by QoS:

1. To create a new QoS mapping:
   a. In the QoS tab, click the **Add QoS** drop-down.  
   b. Select **Create New**.  
   c. Enter a name and description for the QoS mapping.  
   d. Click **Add Queue**. The Add Queue popup displays.  
   e. Select the queue number from the Queue drop-down.  
   f. Select the maximum bandwidth and buffer percentages, and the scheduling and drop types. Enter the forwarding class.  
   g. Click **Save**.  

2. To import an existing QoS mapping:
   a. In the QoS tab, click the **Add QoS** drop-down.  
   b. Select **Import Existing**.  
   c. Select a QoS mapping.  
   d. Click **Import**.  

3. To view or copy a QoS mapping or to remove the mapping from the localized policy, click the **More Actions** icon to the right of the row, and select the desired action.  

4. To configure policy rewrite rules for the QoS mapping:
a. In the QoS tab, click the Add Rewrite Policy drop-down.

b. Select Create New.

c. Enter a name and description for the rewrite rule.

d. Click Add Rewrite Rule. The Add Rule popup displays.

e. Select a class from the Class drop-down.

f. Select the priority (Low or High) from the Priority drop-down.

g. Enter the DSCP value (0 through 63) in the DSCP field.

h. Enter the class of service (CoS) value (0 through 7) in the Layer 2 Class of Service field.

i. Click Save.

5. To import an existing rewrite rule:

a. In the QoS tab, click the Add Rewrite Policy drop-down.

b. Select Import Existing.

c. Select a rewrite rule.

d. Click Import.

6. Click Next to move to Configure Access Lists in the wizard.

**Step 4: Configure ACLs**

1. In the Configure Access Control Lists screen, configure ACLs.

2. To create a new IPv4 ACL, click the Add Access Control List Policy drop-down. Then select Add IPv4 ACL Policy:

3. Enter a name and description for the ACL.

4. In the left pane, click Add ACL Sequence. An Access Control List box is displayed in the left pane.

5. Double-click the Access Control List box, and type a name for the ACL.

6. In the right pane, click Add Sequence Rule to create a single sequence in the ACL. The Match tab is selected by default.

7. Click a match condition.

8. On the left, enter the values for the match condition.

9. On the right enter the action or actions to take if the policy matches.

10. Repeat Steps 6 through 8 to add match–action pairs to the ACL.

11. To rearrange match–action pairs in the ACL, in the right pane drag them to the desired position.

12. To remove a match–action pair from the ACL, click the X in the upper right of the condition.

13. Click Save Match and Actions to save a sequence rule.
14. To rearrange sequence rules in an ACL, in the left pane drag the rules to the desired position.

15. To copy, delete, or rename an ACL sequence rule, in the left pane, click More Options next to the rule's name and select the desired option.

16. If no packets match any of the ACL sequence rules, the default action is to drop the packets. To change the default action:
   a. Click Default Action in the left pane.
   b. Click the Pencil icon.
   c. Change the default action to Accept.
   d. Click Save Match and Actions.

17. Click Next to move to Configure Route Policy in the wizard.

18. Click Next to move to the Policy Overview screen.

**Step 5: Configure Policy Settings**

In Policy Overview, configure policy settings:

1. Enter a name and description for the ACL.

2. To enable cflowd visibility so that a Cisco vEdge device or a Cisco XE SD-WAN device can perform traffic flow monitoring on traffic coming to the router from the LAN, click Netflow.

3. To enable application visibility so that a Cisco vEdge device or a Cisco XE SD-WAN device can monitor and track the applications running on the LAN, click Application.

4. To enable QoS scheduling and shaping for traffic that a vEdge Cloud router receives from transport-side interfaces, click Cloud QoS.

5. To enable QoS scheduling and shaping for traffic that a vEdge Cloud router receives from service-side interfaces, click Cloud QoS Service Side.

6. To log the headers of all packets that are dropped because they do not match a service configured by an Allow Service parameter on a tunnel interface, click Implicit ACL Logging.

7. To configure how often packets flows are logged, click Log Frequency. Packet flows are those that match an access list (ACL), a cflowd flow, or an application-aware routing flow.

8. Click Preview to view the full policy in CLI format.

9. Click Save Policy.

**Step 6: Apply a Localized Data Policy in a Device Template**

1. In the Cisco vManage NMS, select the Configuration > Templates screen.

2. If you are creating a new device template:
   a. In the Device tab, click Create Template.
   b. From the Create Template drop-down, select From Feature Template.
c. From the Device Model drop-down, select one of the Cisco vEdge devices or one of the Cisco XE SD-WAN devices.

d. In the Template Name field, enter a name for the device template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores (_). It cannot contain spaces or any other characters.

e. In the Description field, enter a description for the device template. This field is mandatory, and it can contain any characters and spaces.

f. Continue with Step 4.

3. If you are editing an existing device template:
   a. In the Device tab, click the More Actions icon to the right of the desired template, and click the Pencil icon.
   b. Click the Additional Templates tab. The screen scrolls to the Additional Templates section.
   c. From the Policy drop-down, select the name of a policy that you have configured.

4. Click the Additional Templates tab located directly beneath the Description field. The screen scrolls to the Additional Templates section.

5. From the Policy drop-down, select the name of the policy you configured in the above procedure.

6. Click Create (for a new template) or Update (for an existing template).

Structural Components of Configuration for Access Lists

Following are the structural components required to configure access lists, shown as they appear in the CLI and when you click Preview in the Cisco vManage localized policy configuration wizard. Each component is explained in the sections below.

```
policy
  lists
    data-prefix-list list-name
    ip-prefix prefix/length
  class-map
    class class map map
  cloud-qos
  cloud-qos-service-side
  implicit-acl-logging
  log-frequency number
  qos-scheduler scheduler-name
    class class-name
    bandwidth-percent percentage
    buffer-percent percentage
    drops drop-type
    scheduling (llq | wrr)
  qos-map map-name
    qos-scheduler scheduler-name
  rewrite-rule rule-name
    class class-name priority dscp dscp-value layer-2-cos number
    remote-dest ip-address source ip-address
  policer policer-name
    rate bandwidth
    burst bytes
    exceed action
  access-list list-name
```
Lists

Access lists use prefix lists to group related prefixes.

In the Cisco vManage NMS, you configure prefix lists from:

- Configuration > Policies > Localized Policy > Add Policy > Create Groups of Interest
- Configuration > Policies > Custom Options > Localized Policy > Lists > Data Prefix

In the CLI, you configure lists under the policy lists command hierarchy on Cisco devices.

<table>
<thead>
<tr>
<th>List Type</th>
<th>Description</th>
<th>vManage Configuration/ CLI Configuration Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data prefixes</td>
<td>List of one or more IP prefixes. You can specify both unicast and multicast addresses. To configure multiple prefixes in a single list, include multiple ip-prefix options, specifying one prefix in each option.</td>
<td>Configuration &gt; Policies &gt; Localized Policy &gt; Add Policy &gt; Create Groups of Interest &gt; Data Prefix &gt; New Data Prefix List</td>
</tr>
<tr>
<td></td>
<td>data-prefix-list list-name ip-prefix prefix/length</td>
<td>data-prefix-list list-name ip-prefix prefix/length</td>
</tr>
</tbody>
</table>

**Logging Parameters**

If you configure a logging action in a data policy, by default, the Cisco vEdge devices log all data packet headers to a syslog file. You can log only a sample of the data packet headers.

In the Cisco vManage NMS, you configure how often to log packet headers from:

- Configuration > Policies > Localized Policy > Add Policy > Policy Overview > Log Frequency field

In the CLI, you configure this as follows:

```
vEdge(config)＃policy log-frequency number
```
number specifies how often to log packet headers. The default value is 1000. number can be an integer, and the software rounds the value down to the nearest power of 2. So for example, with the default value of 1000, the logging frequency is rounded down to 512, so every 512th packet is logged.

You can log the headers of all packets that are dropped because they do not match a service configured with an Allow Service configuration or an allow-service command. You can use these logs for security purposes, for example, to monitor the flows that are being directed to a WAN interface and to determine, in the case of a DDoS attack, which IP addresses to block.

In the Cisco vManage NMS, you configure this logging from:

- Configuration > Policies > Localized Policy > Add Policy > Policy Overview > Implicit ACL Logging field

In the CLI, you do this as follows:

vEdge(config)# policy implicit-acl-logging

When you enable implicit ACL logging, by default, the headers of all dropped packets are logged. It is recommended that you configure a limit to the number of packets logged in the Log Frequency field or with the log-frequency command.

**Mirroring Parameters**

To configure mirroring parameters, define the remote destination to which to mirror the packets, and define the source of the packets.

In Cisco vManage NMS, you configure mirroring parameters from:

- Configuration > Policies > Localized Policy > Add Policy > Create Groups of Interest > Mirror > New Mirror List

- Configuration > Policies > Custom Options > Localized Policy > Lists > Mirror > New Mirror List

In the CLI, you configure mirroring parameters as follows:

vEdge(config)# policy mirror
mirror-name
source
remote-dest ip-address
ip-address

Mirroring applies to unicast traffic only. It does not apply to multicast traffic.

**Control Traffic Flow Using Class of Service Values**

**Table 16: Feature History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco SD-WAN 19.2</td>
<td>Feature introduced. This feature lets you control the flow of traffic into and out of a Cisco vEdge device's interface based on the conditions defined in the quality of service (QoS) map. A priority field and a layer 2 class of service (CoS) were added for configuring the re-write rule.</td>
</tr>
</tbody>
</table>
QoS Parameters

In the Cisco vManage NMS, you configure QoS parameters on Cisco vEdge devices and Cisco XE SD-WAN devices from:

- Configuration > Policies > Localized Policy > Add Policy > Create Groups of Interest > Class Map, or Configuration > Policies > Custom Options > Localized Policy > Lists > Class Map
- Configuration > Policies > Localized Policy > Add Policy > Configuring Forwarding Classes/QoS, or Configuration > Policies > Custom Options > Localized Policy > Configuring Forwarding Classes/QoS
- Configuration > Policies > Localized Policy > Add Policy > Policy Overview, or Configuration > Policies > Custom Options > Localized Policy > Policy Overview

This section explains how to configure QoS parameters from the CLI.

To configure QoS parameters on a Cisco vEdge device or a Cisco XE SD-WAN device, first define a classification. In Cisco vManage NMS:

```
vEdge(config)# policy class-map class class-name queue number
```

* class-name is the name of the class. It can be a text string from 1 through 32 characters long.

For hardware, each interface has eight queues, numbered from 0 through 7. Queue 0 is reserved for low-latency queuing (LLQ), so any class that is mapped to queue 0 must be configured to use LLQ. The default scheduling method for all is weighted round-robin (WRR).

For Cisco vEdge Cloud devices, each interface has four queues, numbered from 0 through 3. Queue 0 is reserved for control traffic, and queues 1, 2, and 3 are available for data traffic. The scheduling method for all four queues is WRR. LLQ is not supported.

To configure QoS parameters on a Cisco vEdge Cloud device, you must enable QoS scheduling and shaping. To enable QoS parameters for traffic that the Cisco vEdge Cloud device receives from transport-side interfaces:

```
vEdgeCloud(config)# policy cloud-qos
```

To enable QoS parameters for traffic that the Cisco vEdge Cloud device receives from service-side interfaces:

```
vEdgeCloud(config)# policy cloud-qos-service-side
```

Next, configure scheduling:

```
vEdge(config)# policy qos-scheduler scheduler-name
vEdge(config-qos-scheduler)# class percentage
vEdge(config-qos-scheduler)# buffer-percent percentage
vEdge(config-qos-scheduler)# drops (red-drop | tail-drop)
vEdge(config-qos-scheduler)# scheduling (llq | wrr)
```

* scheduler-name is the name of the QoS scheduler. It can be a text string from 1 through 32 characters long.

* class-name is the name of the forwarding class and can be a text string from 1 through 32 characters long.

The common class names correspond to the per-hop behaviors AF (assured forwarding), BE (best effort), and EF (expedited forwarding).

The bandwidth percentage is the percentage of the interface's bandwidth to allocate to the forwarding class. The sum of the bandwidth on all forwarding classes on an interface should not exceed 100 percent.

The buffer percentage is the percentage of the interface's buffering capacity to allocate to the forwarding class. The sum of the buffering capacity of all forwarding classes on an interface should not exceed 100 percent.
Packets that exceed the bandwidth or buffer percentage are dropped either randomly, using random early detection (red-drop), or from the end of the queue (tail-drop). Low-latency queuing (LLQ) cannot use random early detection.

The algorithm to schedule interface queues can be either low-latency queuing (llq) or weighted round-robin (wrr).

Then, assign the scheduler to a QoS map:

```
vEdge(config-policy)# qos-map map-name qos-scheduler scheduler-name
```

`map-name` is the name of the QoS map, and `scheduler-name` is the name of the scheduler you configured above. Each name can be a text string from 1 through 32 characters long.

Finally, to configure a rewrite rule to overwrite the DSCP field of a packet's outer IP header:

```
vEdge(config)# policy rewrite-rule rule-name class class-name loss-priority
dscp dscp-value layer-2-cos number
```

`rule-name` is the name of the rewrite rule. It can be a text string from 1 through 32 characters long.

`class-name` is the name of a class you configured with the `qos-scheduler class` command. The packet loss priority (PLP) can be either `high` or `low`. To have a DSCP value overwrite the DSCP field of the packet's outer IP header, set a value from 0 through 63. To include an 802.1p marking in the packet, specify a number from 0 through 7.

**Policer Parameters**

To configure policing parameters, create a policer that specifies the maximum bandwidth and burst rate for traffic on an interface, and how to handle traffic that exceeds these values.

In the Cisco vManage NMS, you configure policer parameters from:

- Configuration > Policies > Centralized Policy > Add Policy > Create Groups of Interest > Policer
- Configuration > Policies > Custom Options > Centralized Policy > Lists > Policer

In the CLI, you configure policer parameters as follows:

```
vSmart(config)# policy policer policer-name
vSmart(config-policer)# rate bps
vSmart(config-policer)# burst bytes
vSmart(config-policer)# exceed action
```

`rate` is the maximum traffic rate. It can be a value from 0 through 264 – 1 bits per second.

`burst` is the maximum traffic burst size. It can be a value from 15000 to 1000000 bytes.

`exceed` is the action to take when the burst size or traffic rate is exceeded. `action` can be `drop` (the default) or `remark`. The `drop` action is equivalent to setting the packet loss priority (PLP) bit to low. The `remark` action sets the PLP bit to high. In centralized data policy, access lists, and application-aware routing policy, you can match the PLP with the `match plp` option.

**Sequences**

An access list contains sequences of match–action pairs. The sequences are numbered to set the order in which a packet is analyzed by the match–action pairs in the access lists.

In the Cisco vManage NMS, you configure sequences from:

- Configuration > Policies > Localized Policy > Add Policy > Configure Access Control Lists > Add Access Control List Policy > Add ACL Sequence
In the CLI, you configure sequences with the **policy access-list sequence** command. Each sequence in an access list can contain one match condition and one action condition.

### Match Parameters

Access lists can match IP prefixes and fields in the IP headers.

In the Cisco vManage NMS, you configure match parameters from:

- **Configuration > Policies > Localized Policy > Add Policy > Configure Access Control Lists > Add Access Control List Policy > Add ACL Sequence > Add Sequence Rule > Match**
- **Configuration > Policies > Custom Options > Localized Policy > Access Control List Policy > Add Access Control List Policy > Add ACL Sequence > Add Sequence Rule > Match**

In the CLI, you configure the match parameters with the **policy access-list sequence match** command. Each sequence in an access-list must contain one match condition. For access lists, you can match these parameters:

**Table 17:**

<table>
<thead>
<tr>
<th>Description</th>
<th>vManage Configuration/ CLI Configuration Command</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classification map</td>
<td>Match Class</td>
<td>Name of a class defined with a <strong>policy class-map</strong> command.</td>
</tr>
<tr>
<td></td>
<td>class class-name</td>
<td></td>
</tr>
<tr>
<td>Group of destination prefixes</td>
<td>Match Destination Data Prefix</td>
<td>Name of a <strong>data-prefix-list</strong> list.</td>
</tr>
<tr>
<td></td>
<td>destination-data-prefix-list list-name</td>
<td></td>
</tr>
<tr>
<td>Individual destination prefix</td>
<td>Not available in vManage NMS</td>
<td>IP prefix and prefix length</td>
</tr>
<tr>
<td></td>
<td>destination-ip prefix/length</td>
<td></td>
</tr>
<tr>
<td>Destination port number</td>
<td>Match Destination Port</td>
<td>0 through 65535; specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-])</td>
</tr>
<tr>
<td></td>
<td>destination-port number</td>
<td></td>
</tr>
<tr>
<td>DSCP value</td>
<td>Match DSCP</td>
<td>0 through 63</td>
</tr>
<tr>
<td></td>
<td>dscp number</td>
<td></td>
</tr>
<tr>
<td>Internet Protocol number</td>
<td>Match Protocol</td>
<td>0 through 255</td>
</tr>
<tr>
<td></td>
<td>protocol number</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>vManage Configuration/ CLI Configuration Command</td>
<td>Value or Range</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Packet length</td>
<td>Match Packet Length packet-length number</td>
<td>Length of the packet. <em>number</em> can be from 0 through 65535. Specify a single length, a list of lengths (with numbers separated by a space), or a range of lengths (with the two numbers separated with a hyphen [-])</td>
</tr>
<tr>
<td>Group of source prefixes</td>
<td>Match Source Data Prefix source-data-prefix-list list-name</td>
<td>Name of a data-prefix-list list.</td>
</tr>
<tr>
<td>Packet loss priority (PLP)</td>
<td>Match PLP plp</td>
<td>(high</td>
</tr>
<tr>
<td>Individual source prefix</td>
<td>Match Source Data Prefix source-ip prefix/length</td>
<td>IP prefix and prefix length</td>
</tr>
<tr>
<td>Source port number .</td>
<td>Match Source Port source-port address</td>
<td>0 through 65535; specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-])</td>
</tr>
<tr>
<td>TCP flag</td>
<td>Match TCP tcp flag</td>
<td>syn</td>
</tr>
</tbody>
</table>

**Action Parameters**

When a packet matches the conditions in the match portion of an access list, the packet can be accepted or dropped, and it can be counted. Then, you can classify, mirror, or police accepted packets.

In the Cisco vManage NMS, you configure match parameters from:

- **Configuration > Policies > Localized Policy > Add Policy > Configure Access Control Lists > Add Access Control List Policy > Add ACL Sequence > Add Sequence Rule > Action**

- **Configuration > Policies > Custom Options > Localized Policy > Access Control List Policy > Add Access Control List Policy > Add ACL Sequence > Add Sequence Rule > Action**

In the CLI, you configure the actions parameters with the **policy access-list sequence action** command.

Each sequence in an access list can contain one action condition.

In the action, you first specify whether to accept or drop a matching data packet, and whether to count it:
Table 18:

<table>
<thead>
<tr>
<th>Description</th>
<th>vManage Configuration/ CLI Configuration Parameter</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept the packet. An accepted packet is eligible to be modified by the additional parameters configured in the action portion of the access list.</td>
<td>Click Accept accept</td>
<td>—</td>
</tr>
<tr>
<td>Count the accepted or dropped packets.</td>
<td>Action Counter Click Accept, then action Counter count counter-name</td>
<td>Name of a counter. To display counter information, use the show policy access-lists counters command on the Cisco device.</td>
</tr>
<tr>
<td>Discard the packet. This is the default action.</td>
<td>Click Drop drop</td>
<td>—</td>
</tr>
<tr>
<td>Log the packet headers into the messages and vsyslog system logging (syslog) files. In addition to logging the packet headers, a syslog message is generated the first time a packet header is logged and then every 5 minutes thereafter, as long as the flow is active.</td>
<td>Action Log Click Accept, then action Log log</td>
<td>To display logging information, use the show app log flow-all, show app log flows, and show log commands on the Cisco vEdge device.</td>
</tr>
</tbody>
</table>

For a packet that is accepted, the following actions can be configured:

Table 19:

<table>
<thead>
<tr>
<th>Description</th>
<th>vManage Configuration/ CLI Configuration Parameter</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classify the packet.</td>
<td>Click Accept, then Class class class-name</td>
<td>Name of a QoS class defined with a policy class-map command.</td>
</tr>
<tr>
<td>Mirror the packet.</td>
<td>Click Accept, then Mirror List mirror mirror-name</td>
<td>Name of mirror defined with a policy mirror command.</td>
</tr>
<tr>
<td>Police the packet.</td>
<td>Click Accept, then Policer policer policer-name</td>
<td>Name of a policer defined with a policy policer command.</td>
</tr>
<tr>
<td>Packet's DSCP value.</td>
<td>Click Accept, then DSCP set dscp value</td>
<td>0 through 63.</td>
</tr>
<tr>
<td>Next-hop address.</td>
<td>Click Accept, then Next Hop set next-hop ipv4-address</td>
<td>IPv4 address.</td>
</tr>
</tbody>
</table>
**Default Action**

If a packet being evaluated does not match any of the match conditions in a access list, a default action is applied to this packet. By default, the packet is dropped.

In the Cisco vManage NMS, you modify the default action from:

- **Configuration > Policies > Localized Policy > Add Policy > Configure Access Control Lists > Default Action**
- **Configuration > Policies > Custom Options > Localized Policy > Access Control List Policy > Default Action**

In the CLI, you modify this behavior with the `access-list default-action accept` command.

**Apply Access Lists**

For an access list to take effect, you must apply it to an interface.

In the Cisco vManage NMS, you apply the access list in one of these interface feature configuration templates:

- **Configuration > Templates > VPN Interface Bridge**
- **Configuration > Templates > VPN Interface Cellular**
- **Configuration > Templates > VPN Interface Ethernet**
- **Configuration > Templates > VPN Interface GRE**
- **Configuration > Templates > VPN Interface PPP**
- **Configuration > Templates > VPN Interface PPP Ethernet**

In the CLI, you apply the access list as follows:

```
vEdge(config)# vpn vpn-id interface interface-name
vEdge(config-interface)# access-list list-name (in | out)
```

Applying the policy in the inbound direction (in) affects prefixes being received on the interface. Applying it in the outbound direction (out) affects prefixes being transmitted on the interface.

For an access list that applies QoS classification, apply any DSCP rewrite rules to the same interface to which you apply the access list:

```
vEdge(config)# vpn vpn-id interface interface-name rewrite-rule rule-name
```

Note that you can also apply a policer directly to an interface, which has the effect of policing all packets transiting the interface, rather than policing only the selected packets that match the access list. You can apply the policer to either inbound or outbound packets:

```
vEdge(config)# vpn vpn-id interface interface-name
vEdge(config-interface)# policer
policer-name (in | out) interface-name
```

**Explicit and Implicit Access Lists**

Access lists that you configure through localized data policy using the `policy access-list` command are called **explicit ACLs**. You can apply explicit ACLs to any interface in any VPN on the router.

The router's tunnel interfaces in VPN 0 also have **implicit ACLs**, which are also referred to as **services**. Some services are enabled by default on the tunnel interface, and are in effect unless you disable them. Through
configuration, you can also enable other services. You configure and modify implicit ACLs with the `allow-service` command:

```
veEdge(config)# vpn 0
veEdge(config-vpn)# interface interface-name
veEdge(config-interface)# tunnel-interface
veEdge(config-tunnel-interface)# allow-service service-name
veEdge(config-tunnel-interface)# no allow-service service-name
```

On Cisco devices, the following services are enabled by default: DHCP (for DHCPv4 and DHCPv6), DNS, and ICMP. These three services allow the tunnel interface to accept DHCP, DNS, and ICMP packets. You can also enable services for BGP, Netconf, NTP, OSPF, SSHD, and STUN.

When data traffic matches both an explicit ACL and an implicit ACL, how the packets are handled depends on the ACL configuration. Specifically, it depends on:

- Whether the implicit ACL is configured as allow (`allow-service allow-service`) or deny (`no allow-service service-name`). Allowing a service in an implicit ACL is the same as specifying the `accept` action in an explicit ACL, and a service that is not allowed in an implicit ACL is the same as specifying the `drop` action in an explicit ACL.

- Whether, in an explicit ACL, the `accept` or `deny` action is configured in a policy sequence or in the default action.

The following table explains how traffic matching both an implicit and an explicit ACL is handled:

<table>
<thead>
<tr>
<th>Implicit ACL</th>
<th>Explicit ACL: Sequence</th>
<th>Explicit ACL: Default</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow (accept)</td>
<td>Deny (drop)</td>
<td>—</td>
<td>Deny (drop)</td>
</tr>
<tr>
<td>Allow (accept)</td>
<td>—</td>
<td>Deny (drop)</td>
<td>Allow (accept)</td>
</tr>
<tr>
<td>Deny (drop)</td>
<td>Allow (accept)</td>
<td>—</td>
<td>Allow (accept)</td>
</tr>
<tr>
<td>Deny (drop)</td>
<td>—</td>
<td>Allow (accept)</td>
<td>Deny (drop)</td>
</tr>
</tbody>
</table>

**Configure Localized Data Policy for IPv4 Using the CLI for Cisco vEdge Devices**

Following are the high-level steps for configuring an access list using the CLI for Cisco vEdge devices:

1. Create lists of IP prefixes, as needed:

   ```
   veEdge(config)# policy
   veEdge(config-policy)# lists data-prefix-list list-name
   veEdge(config-data-prefix-list)# ip-prefix prefix/length
   ```

2. If you configure a logging action, configure how often to log packets to the syslog files:

   ```
   veEdge(config)# policy log-frequency number
   ```

3. For QoS, map each forwarding class to an output queue, configure a QoS scheduler for each forwarding class, and group the QoS schedulers into a QoS map:
vEdge(config)# policy class-map
vEdge(config-class-map)# class class-name queue number
vEdge(config)# policy qos-scheduler scheduler-name
vEdge(config-qos-scheduler)# class class-name
vEdge(config-qos-scheduler)# bandwidth-percent percentage
vEdge(config-qos-scheduler)# buffer-percent percentage
vEdge(config-qos-scheduler)# drops drop-type
vEdge(config-qos-scheduler)# scheduling type

vEdge(config)# policy qos-map map-name qos-scheduler scheduler-name

4. For QoS, define rewrite rules to overwrite the DSCP field of a packet's outer IP header, if desired:

vEdge(config)# policy rewrite-rule rule-name
vEdge(config-rewrite-rule)# class class-name loss-priority
dscp dscp-value layer-2-cos number

class-name is one of the classes defined under a qos-scheduler command.

5. Define mirroring parameters (for unicast traffic only):

vEdge(config)# policy mirror mirror-name
vEdge(config-mirror)# remote-dest ip-address source ip-address

6. Define policing parameters:

vEdge(config)# policy policer policer-name
vEdge(config-policer)# rate bandwidth
vEdge(config-policer)# burst bytes
vEdge(config-policer)# exceed action

7. Create an access list instance:

vEdge(config)# policy access-list list-name

8. Create a series of match–action pair sequences:

vEdge(config-access-list)# sequence number
vEdge(config-sequence)#

The match–action pairs are evaluated in order, by sequence number, starting with the lowest numbered pair and ending when the route matches the conditions in one of the pairs. Or if no match occurs, the default action is taken (either rejecting the route or accepting it as is).

9. Define match parameters for packets:

vEdge(config-sequence-number)
# match match-parameter

10. Define actions to take when a match occurs:

vEdge(config-sequence)# action drop
vEdge(config-sequence)# action count counter-name
vEdge(config-sequence)# action log
vEdge(config-sequence)# action accept class class-name
vEdge(config-sequence)# action accept mirror mirror-name
vEdge(config-sequence)# action accept policer policer-name
vEdge(config-sequence)# action accept set dscp value
vEdge(config-sequence)# action accept set next-hop ipv4-address

11. Create additional numbered sequences of match–action pairs within the access list, as needed.

12. If a packet does not match any of the conditions in one of the sequences, it is rejected by default. If you want nonmatching packets to be accepted, configure the default action for the access list:
vEdge(config-policy-name)
  # default-action accept

13. Apply the access list to an interface:

vEdge(config)# vpn vpn-id interface interface-name
vEdge(config-interface)# access-list list-name (in | out)

Applying the access list in the inbound direction (in) affects packets being received on the interface. Applying it in the outbound direction (out) affects packets being transmitted on the interface. For QoS, apply a DSCP rewrite rule to the same egress interface:

vEdge(config)# vpn vpn-id interface interface-name rewrite-rule rule-name

14. You can apply a policer directly to an interface, which has the effect of policing all packets transiting the interface, rather than policing only the selected packets that match the access list. You can apply the policer to either inbound or outbound packets:

vEdge(config)# vpn vpn-id interface interface-name
vEdge(config-interface)# policer policer-name (in | out)

Localized Data Policy for IPv6

This topic provides procedures for configuring IPv6 localized data policy. This type of data policy is called access lists, or ACLs. You can provision simple access lists that filter traffic based on IP header fields. You also use access lists to apply mirroring and policing to data packets.

For IPv6, you can apply access lists only to interfaces in the transport VPN, VPN 0.

In the Cisco vManage NMS, you configure localized data policy from the Configuration > Policies screen, using a policy configuration wizard. In the CLI you configure these policies on the Cisco device.

Configuration Components

An access list consists of a sequences of match–action pairs that are evaluated in order, from lowest sequence number to highest sequence number. When a packet matches one of the match conditions, the associated action is taken and policy evaluation on that packets stops. Keep this in mind as you design your policies to ensure that the desired actions are taken on the items subject to policy.

If a packet matches no parameters in any of the sequences in the policy configuration, it is, by default, dropped.

The following figure illustrates the configuration components for IPv6 access lists:
Configure Localized Data Policy for IPv6 Using Cisco vManage

To configure IPv6 localized data policy, use the Cisco vManage policy configuration wizard. The wizard is a UI policy builder that consists of five screens, and you use four of them to configure IPv6 localized policy components:

• Groups of Interest, also called *lists*—Create data prefix lists, mirroring, and policer parameters that group together related items and that you call in the match or action components of a policy.

• Access Control Lists—Define the match and action conditions of ACLs.

• Route Policies—Define the match and action conditions of route policies.

• Policy Settings—Define additional policy settings.

  Define the frequency for logging policy-related packet headers.

You configure some or all these components depending on the specific policy you are creating. To skip a component, click the Next button at the bottom of the screen. To return to a component, click the Back button at the bottom of the screen.

**Step 1: Start the Policy Configuration Wizard**

To start the policy configuration wizard:

1. In the Cisco vManage NMS, select the **Configure > Policies** screen. When you first open this screen, the Centralized Policy tab is selected by default.

2. Select the **Localized Policy** tab.

3. Click **Add Policy**. The policy configuration wizard opens, and the Create Groups of Interest screen is displayed.

**Step 2: Create Groups of Interest**

In the Create Groups of interest screen create lists to use in the localized data policy:
1. Create new lists of groups, as described in the following table:

<table>
<thead>
<tr>
<th>List Type</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| AS Path   | Permit or deny prefixes from certain autonomous systems.  
   a. In the left bar, click **AS Path**.  
   b. Enter a name for the list.  
      1. For Cisco devices: Enter an alphanumeric value.  
      2. For Cisco ISR Edge devices: Enter a number from 1 to 500.  
   c. Set the preference value for the list in the **Add AS Path** field. |
| Community | a. In the left bar, click **Community**.  
   b. Click **New Community List**.  
   c. Enter a name for the list.  
   d. In the **Add Community** field, enter one or more data prefixes separated by commas.  
   e. Click **Add**. |
<table>
<thead>
<tr>
<th>List Type</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| Data Prefix                | a. In the left bar, click **Data Prefix**.  
 |                            | b. Click **New Data Prefix List**.  
 |                            | c. Enter a name for the list.  
 |                            | d. In the Internet Protocol field, click **IPv4** or **IPv6**.  
 |                            | e. In the **Add Data prefix** field, enter one or more data prefixes separated by commas.  
 |                            | f. Click **Add**.  |
| Extended Community         | a. In the left bar, click **Extended Community**.  
 |                            | b. Click **New Extended Community List**.  
 |                            | c. Enter a name for the list.  
 |                            | d. In the **Add Extended Community** field, enter one or more data prefixes separated by commas.  
 |                            | e. Click **Add**.  |
| Class Map                  | Map a class name to an interface queue number.  
 |                            | a. In the left bar, click **Class Map**.  
 |                            | b. Click **New Class List**. The Class List popup displays.  
 |                            | c. Enter a name for the list. The class name can be a text string from 1 to 32 characters long.  
 |                            | d. Select a queue number between 0 and 7 from the **Queue** drop-down menu.  
 |                            | e. Click **Save**.  |
| Mirror                     | Define the remote destination for mirrored packets, and define the source of the packets.  
 |                            | a. In the left bar, click **Mirror**.  
 |                            | b. Click **New Mirror List**.  
 |                            | c. Enter a name for the list.  
 |                            | d. Enter the **Remote Destination IP** address in the left field, where the mirrored traffic should be routed.  
 |                            | e. Enter the **Source IP** address of the mirrored traffic in the right field.  
<p>|                            | f. Click <strong>Add</strong>. |</p>
<table>
<thead>
<tr>
<th>List Type</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| Policer   | a. In the left bar, click Policer.  
             b. Click New Policer List.  
             c. Enter a name for the list.  
             d. Define the policing parameters:  
                1. In the Burst field, enter the maximum traffic burst size, a value from 15,000 to 10,000,000 bytes.  
                2. In the Exceed field, select the action to take when the burst size or traffic rate is exceeded. It can be drop, which sets the packet loss priority (PLP) to low, or remark, which sets the PLP to high.  
                3. In the Rate field, enter the maximum traffic rate, a value from 0 through 264 – 1 bits per second (bps).  
             e. Click Add. |
| Prefix    | a. In the left bar, click Prefix.  
             b. Click New Prefix List.  
             c. Enter a name for the list.  
             d. Click either IPv4 or IPv6.  
             e. Under Add Prefix, enter the prefix for the list. (An example is displayed.) Optionally, click the green Import link on the right-hand side to import a prefix list.  
             f. Click Add. |

2. Click Next to move to Configure Forwarding Classes/QoS in the wizard. For IPv6 localized data policy, you cannot configure QoS.

3. Click Next to move to Configure Access Lists in the wizard.

**Step 3: Configure ACLs**

1. In the Configure Access Control Lists screen, click Add Access Control List Policy, and choose Add IPv6 ACL Policy from the drop-down.

2. Enter a name and description for the ACL.

3. From the left column, click Add ACL Sequence.

4. Click Sequence Rule to open the ACL match/action sequence menu.

5. Click a match condition. See Match Parameters for a full description of these options.

6. On the left side, enter the values for the match condition.
7. On the right side, enter the action or actions to take if the policy matches. See Action Parameters for a full description of these options.

8. Repeat Steps 3 through 7 to add match–action pairs to the ACL.

9. To rearrange match–action pairs in the ACL, drag them to the desired position in the right pane.

10. To remove a match–action pair from the ACL, click the X in the upper right of the condition.

11. Click Save Match and Actions to save a sequence rule.

12. To copy, delete, or rename an ACL sequence rule, in the left pane, click the More Options menu (three dots) next to the rule's name and select the desired option.

13. If no packets match any of the ACL sequence rules, the default action is to drop the packets. To change the default action:
   a. Click Default Action in the left pane.
   b. Click the Pencil icon.
   c. Change the default action to Accept.
   d. Click Save Match and Actions.

14. Click Next to move to Configure Route Policy in the wizard.

15. Click Next to move to the Policy Overview screen.

Step 4: Configure Policy Settings

In Policy Overview, configure policy settings:

1. Enter a name and description for the ACL.

2. Under Policy Settings, select one of the following policy options:

<table>
<thead>
<tr>
<th>Policy Settings Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Netflow</td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td></td>
</tr>
<tr>
<td>Cloud QoS</td>
<td></td>
</tr>
<tr>
<td>Cloud QoS Service side</td>
<td></td>
</tr>
<tr>
<td>Implicit ACL Logging</td>
<td>Log the headers of all packets that are dropped because they do not match a service configured by an Allow Service parameter on a tunnel interface.</td>
</tr>
<tr>
<td>Log Frequency</td>
<td>Configure how often packet flows are logged. Packet flows are those that match an access list (ACL), a cflowd flow, or an application-aware routing flow.</td>
</tr>
</tbody>
</table>

3. Click Preview to view the full policy in CLI format.
4. Click **Save Policy**.

**Step 5: Apply a Localized Data Policy in a Device Template**

1. In the Cisco vManage NMS, select the **Configuration > Templates** screen.

2. If you are creating a new device template:
   a. In the Device tab, click **Create Template**.
   b. From the Create Template drop-down, select **From Feature Template**.
   c. From the **Device Model** drop-down, select a Cisco device.
   d. In the **Template Name** field, enter a name for the device template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores (_). It cannot contain spaces or any other characters.
   e. In the **Description** field, enter a description for the device template. This field is mandatory, and it can contain any characters and spaces.
   f. Continue with Step 4.

3. If you are editing an existing device template:
   a. In the **Device** tab, click the **More Actions** icon to the right of the desired template, and click the pencil icon.
   b. Click the **Additional Templates** tab. The screen scrolls to the Additional Templates section.
   c. From the Policy drop-down, select the name of a policy that you have configured.

4. Click the **Additional Templates** tab located directly beneath the **Description** field. The screen scrolls to the Additional Templates section.

5. From the Policy drop-down, select the name of the policy you configured in the above procedure.

6. Click **Create** (for a new template) or **Update** (for an existing template).

**Structural Components of Configuration for Access Lists**

Following are the structural components required to configure access lists. Each one is explained in more detail in the sections below.

```
policy
  implicit-acl-logging
  log-frequency number
  mirror mirror-name
    remote-dest ip-address source ip-address
  policer policer-name
    rate bandwidth
    burst bytes
    exceed action
policy ipv6
  access-list list-name
  sequence number
    match match-parameters
```
Logging Parameters

If you configure a logging action in a data policy, by default, the Cisco vEdge device logs all data packet headers to a syslog file. You can log only a sample of the data packet headers.

In the Cisco vManage NMS, you configure how often to log packet headers from `Configuration > Policies > Localized Policy > Add Policy > Policy Overview > Log Frequency` field.

In the CLI, you configure this as follows:

```
vEdge(config)# policy implicit-acl-logging
```

You can log the headers of all packets that are dropped because they do not match a service configured with an Allow Service configuration or an `allow-service` command. You can use these logs for security purposes, for example, to monitor the flows that are being directed to a WAN interface and to determine, in the case of a DDoS attack, which IP addresses to block.

In the Cisco vManage NMS, you configure this logging from the `Configuration > Policies > Localized Policy > Add Policy > Policy Overview > Implicit ACL Logging` field.

In the CLI, you do this as follows:

```
vEdge(config)# policy implicit-acl-logging
```

When you enable implicit ACL logging, by default, the headers of all dropped packets are logged. It is recommended that you configure a limit to the number of packets logged in the Log Frequency field or with the `log-frequency` command.

Mirroring Parameters

To configure mirroring parameters, define the remote destination to which to mirror the packets, and define the source of the packets.

In the Cisco vManage NMS, you configure mirroring parameters from:

- `Configuration > Policies > Localized Policy > Add Policy > Create Groups of Interest > Mirror > New Mirror List`
- `Configuration > Policies > Custom Options > Localized Policy > Lists > Mirror > New Mirror List`

In the CLI, you configure mirroring parameters as follows:

```
device(config)# policy mirror mirror-name
device(config-mirror)# remote-dest ip-address source ip-address
```
**Policer Parameters**

To configure policing parameters, create a policer that specifies the maximum bandwidth and burst rate for traffic on an interface, and how to handle traffic that exceeds these values.

In the Cisco vManage NMS, you configure policer parameters from:

- **Configuration > Policies > Localized Policy > Add Policy > Create Groups of Interest > Policer > New Policer List**
- **Configuration > Policies > Custom Options > Localized Policy > Lists > Policer > New Policer List**

In the CLI, you configure policer parameters as follows:

```
vEdge(config)# policy policer policer-name
vEdge(config-policer)# rate bps
vEdge(config-policer)# burst bytes
vEdge(config-policer)# exceed action
```

- **rate** is the maximum traffic rate. It can be a value from 0 through $2^{64} - 1$ bits per second.
- **burst** is the maximum traffic burst size. It can be a value from 15000 to 1000000 bytes.
- **exceed** is the action to take when the burst size or traffic rate is exceeded. **action** can be **drop** (the default) or **remark**. The **drop** action is equivalent to setting the packet loss priority (PLP) bit to low. The **remark** action sets the PLP bit to high. In centralized data policy, access lists, and application-aware routing policy, you can match the PLP with the **match plp** option.

**Sequences**

**Sequences**

An access list contains sequences of match–action pairs. The sequences are numbered to set the order in which a packet is analyzed by the match–action pairs in the access lists.

In the Cisco vManage NMS, you configure sequences from:

- **Configuration > Policies > Localized Policy > Add Policy > Configure Access Control Lists > Add Access Control List Policy > Add ACL Sequence**
- **Configuration > Policies > Custom Options > Localized Policy > Access Control List Policy > Add Access Control List Policy > Add ACL Sequence**

In the CLI, you configure sequences with the **policy ipv6 access-list sequence** command.

Each sequence in an access list can contain one match condition and one action condition.

**Match Parameters**

Access lists can match IP prefixes and fields in the IP headers.

In the Cisco vManage NMS, you configure match parameters from:

- **Configuration > Policies > Localized Policy > Add Policy > Configure Access Control Lists > Add Access Control List Policy > Add ACL Sequence > Add Sequence Rule > Match**
- **Configuration > Policies > Custom Options > Localized Policy > Access Control List Policy > Add Access Control List Policy > Add ACL Sequence > Add Sequence Rule > Match**
In the CLI, you configure the match parameters with the **policy ipv6 access-list sequence match** command. Each sequence in an access list must contain one match condition.

For access lists, you can match these parameters:

<table>
<thead>
<tr>
<th>Description</th>
<th>vManage Match Tab / CLI Command</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter a Destination port number.</td>
<td>Destination Port</td>
<td>0 through 65535; specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-])</td>
</tr>
<tr>
<td>Select the Next Header protocol.</td>
<td>Protocol</td>
<td>0 through 255, corresponding to an Internet Protocol number</td>
</tr>
<tr>
<td>Specify the packet length</td>
<td>Packet Length</td>
<td>Length of the packet. <em>number</em> can be from 0 through 65535. Specify a single length, a list of lengths (with numbers separated by a space), or a range of lengths (with the two numbers separated with a hyphen [-])</td>
</tr>
<tr>
<td>Specify the packet loss priority (PLP)</td>
<td>PLP</td>
<td>*(high</td>
</tr>
<tr>
<td>Select a Source data prefix list</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enter a Source port number</td>
<td>Source Port</td>
<td>0 through 65535; specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-])</td>
</tr>
<tr>
<td>Enter a Destination Data Prefix</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td>TCP</td>
<td>syn</td>
</tr>
<tr>
<td>Set the packet's DSCP value</td>
<td>Class</td>
<td>0 through 63</td>
</tr>
<tr>
<td>Traffic class</td>
<td>Traffic Class</td>
<td>0 through 63</td>
</tr>
</tbody>
</table>

**Action Parameters**

When a packet matches the conditions in the match portion of an access list, the packet can be accepted or dropped, and it can be counted. Then, you can classify, mirror, or police accepted packets.

In the Cisco vManage NMS, you configure match parameters from:
In the CLI, you configure the actions parameters with the `policy ipv6 access-list sequence action` command. Each sequence in an access list can contain one action condition.

For a packet that is accepted, the following actions can be configured:

<table>
<thead>
<tr>
<th>Description</th>
<th>Cisco vManage Action Tab / CLI Command</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept the packet. An accepted packet is eligible to be modified by the</td>
<td>Click <strong>Accept. accept</strong></td>
<td>—</td>
</tr>
<tr>
<td>additional parameters configured in the <strong>action</strong> portion of the access list.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Count the accepted or dropped packets.</td>
<td><strong>Counter Name</strong></td>
<td>Name of a counter. To display counter information, use the</td>
</tr>
<tr>
<td></td>
<td><strong>count counter-name</strong></td>
<td><code>show ipv6 policy access-lists counters</code> command on the Cisco device.</td>
</tr>
<tr>
<td>Log the packet headers into system logging (syslog) files.</td>
<td><strong>Log</strong></td>
<td>To display logging information, use the <code>show app log flow-all</code> and `show</td>
</tr>
<tr>
<td></td>
<td></td>
<td>app log flows` command on the vEdge router.</td>
</tr>
<tr>
<td>Designate the next hop router.</td>
<td><strong>Next Hop</strong></td>
<td></td>
</tr>
<tr>
<td>Traffic Class</td>
<td><strong>set traffic-class value</strong></td>
<td>0-63</td>
</tr>
<tr>
<td>Mirror the packet.</td>
<td><strong>Mirror List</strong></td>
<td>Name of mirror defined with a <code>policy mirror</code> command.</td>
</tr>
<tr>
<td></td>
<td><strong>mirror mirror-name</strong></td>
<td></td>
</tr>
<tr>
<td>Set the packet's DSCP value.</td>
<td><strong>Class</strong></td>
<td>0 through 63</td>
</tr>
<tr>
<td>Police the packet.</td>
<td><strong>Policer</strong></td>
<td>Name of a policer defined with a <code>policy policer</code> command.</td>
</tr>
<tr>
<td></td>
<td><strong>policer policer-name</strong></td>
<td></td>
</tr>
<tr>
<td>Discard the packet. This is the default action.</td>
<td><strong>Click Drop. drop</strong></td>
<td>—</td>
</tr>
</tbody>
</table>
Default Action

If a packet being evaluated does not match any of the match conditions in a access list, a default action is applied to this packet. By default, the packet is dropped.

In the Cisco vManage NMS, you modify the default action from:

- Configuration > Policies > Localized Policy > Add Policy > Configure Access Control Lists > Default Action
- Configuration > Policies > Custom Options > Localized Policy > Access Control List Policy > Default Action

In the CLI, you modify this behavior with the `access-list ipv6 default-action accept` command.

Apply Access Lists

For an access list to take effect, you must apply it to a tunnel interface in VPN 0.

In the Cisco vManage NMS, you apply the access list in one of the interface feature configuration templates.

In the CLI, you apply the access list as follows:

```
vEdge(config)# vpn 0 interface interface-name
vEdge(config-interface)# ipv6 access-list list-name (in | out)
```

Applying the policy in the inbound direction (`in`) affects prefixes being received on the interface. Applying it in the outbound direction (`out`) affects prefixes being transmitted on the interface.

Explicit and Implicit Access Lists

Access lists that you configure through localized data policy using the `policy access-list` command are called explicit ACLs. You can apply explicit ACLs to any interface in any VPN on the router.

The router's tunnel interfaces in VPN 0 also have implicit ACLs, which are also referred to as services. Some services are enabled by default on the tunnel interface, and are in effect unless you disable them. Through configuration, you can also enable other services. You configure and modify implicit ACLs with the `allow-service` command:

```
vEdge(config)# vpn 0
vEdge(config-vpn)# interface interface-name
vEdge(config-interface)# tunnel-interface
vEdge(config-tunnel-interface)# allow-service service-name
vEdge(config-tunnel-interface)# no allow-service service-name
```

On Cisco devices, the following services are enabled by default: DHCP (for DHCPv4 and DHCPv6), DNS, and ICMP. These three services allow the tunnel interface to accept DHCP, DNS, and ICMP packets. You can also enable services for BGP, Netconf, NTP, OSPF, SSHD, and STUN.

When data traffic matches both an explicit ACL and an implicit ACL, how the packets are handled depends on the ACL configuration. Specifically, it depends on:

- Whether the implicit ACL is configured as allow (`allow-service allow-service`) or deny (`no allow-service service-name`). Allowing a service in an implicit ACL is the same as specifying the `accept` action in an explicit ACL, and a service that is not allowed in an implicit ACL is the same as specifying the `drop` action in an explicit ACL.
- Whether, in an explicit ACL, the `accept` or `deny` action is configured in a policy sequence or in the default action.
The following table explains how traffic matching both an implicit and an explicit ACL is handled:

<table>
<thead>
<tr>
<th>Implicit ACL</th>
<th>Explicit ACL: Sequence</th>
<th>Explicit ACL: Default</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow (accept)</td>
<td>Deny (drop)</td>
<td>—</td>
<td>Deny (drop)</td>
</tr>
<tr>
<td>Allow (accept)</td>
<td>—</td>
<td>Deny (drop)</td>
<td>Allow (accept)</td>
</tr>
<tr>
<td>Deny (drop)</td>
<td>Allow (accept)</td>
<td>—</td>
<td>Allow (accept)</td>
</tr>
<tr>
<td>Deny (drop)</td>
<td>—</td>
<td>Allow (accept)</td>
<td>Deny (drop)</td>
</tr>
</tbody>
</table>

**Configure Localized Data Policy for IPv6 Using the CLI**

Following are the high-level steps for configuring an access list using the CLI:

1. Define mirroring parameters (for unicast traffic only):
   ```
   vEdge(config)# policy mirror mirror-name
   vEdge(config-mirror)# remote-dest ip-address source ip-address
   ```

2. Define policing parameters:
   ```
   vEdge(config)# policy policer policer-name
   vEdge(config-policer)# rate bandwidth
   vEdge(config-policer)# burst bytes
   vEdge(config-policer)# exceed action
   ```

3. Create an access list instance:
   ```
   vEdge(config)# policy ipv6 access-list list-name
   ```

4. Create a series of match–action pair sequences:
   ```
   vEdge(config-ipv6-access-list)# sequence number
   ```
   The match–action pairs are evaluated in order, by sequence number, starting with the lowest numbered pair and ending when the route matches the conditions in one of the pairs. Or if no match occurs, the default action is taken (either rejecting the route or accepting it as is).

5. Define match parameters for packets:
   ```
   vEdge(config-sequence-number)# match match-parameter
   ```

6. Define actions to take when a match occurs:
   ```
   vEdge(config-sequence)# action drop
   vEdge(config-sequence)# action count counter-name
   vEdge(config-sequence)# action log
   vEdge(config-sequence)# action accept class class-name
   vEdge(config-sequence)# action accept mirror mirror-name
   vEdge(config-sequence)# action accept policer policer-name
   ```

7. Create additional numbered sequences of match–action pairs within the access list, as needed.
8. If a packet does not match any of the conditions in one of the sequences, it is rejected by default. If you want nonmatching packets to be accepted, configure the default action for the access list:

```
vEdge(config-policy-name)# default-action accept
```

9. Apply the access list to an interface:

```
vEdge(config)# vpn vpn-id interface interface-name
vEdge(config-interface)# ipv6 access-list list-name (in | out)
```

Applying the access list in the inbound direction (in) affects packets being received on the interface. Applying it in the outbound direction (out) affects packets being transmitted on the interface.

## Localized Data Policy Configuration Examples

This topic provides some straightforward examples of configuring localized data policy to help you get an idea of how to use policy to influence traffic flow across the Cisco SD-WAN domain. Localized data policy, also known as access lists, is configured directly on the local Cisco device.

### QoS

You can configure quality of service (QoS) to classify data packets and control how traffic flows out of and in to the interfaces on a Cisco device and on the interface queues. For examples of how to configure a QoS policy, see Forwarding and QoS Configuration Examples.

### Mirroring Example

This example illustrates how to configure a mirror instance to automatically send a copy of certain types of data packet to a specified destination for analysis. After you configure the mirror instance, include it in an access list. Here, "mirror-m1" is configured with the host at source address 10.20.23.16 and destination host at 10.2.2.11. The mirror instance is then included in the access list "acl2," which is configured so that data packets originating from the host at source address 10.20.24.17 and going to the destination host at 10.20.25.18 are mirrored to the destination host at 10.2.2.11 with the source address of the originating host as 10.20.23.16.

```
policy
  mirror m1
      remote-dest 10.2.2.11 source 10.20.23.16
!
!
vm5# show running-config policy access-list acl2
policy
  access-list acl2
    sequence 1
      match
        source-ip 10.20.24.17/32
        destination-ip 10.20.25.18/32
      action accept
      mirror m1
!
  default-action drop
!```
CHAPTER 6

Policy Basics CLI Reference

CLI commands for configuring and monitoring policy.

Centralized Control Policy Command Hierarchy

Configure on Cisco vSmart Controllers only.

```plaintext
policy
lists
color-list list-name
color color
prefix-list list-name
ip-prefix prefix/length
site-list list-name
site-id site-id
tloc-list list-name
tloc address color color encap encapsulation [preference value weight value]
vpn-list list-name
vpn vpn-id

policy
control-policy policy-name
default-action action
sequence number
match
route
color color
color-list list-name
omp-tag number
origin protocol
originator ip-address
preference number
prefix-list list-name
site-id site-id
site-list list-name
tloc address
tloc-list list-name
vpn vpn-id
vpn-list list-name
tloc
carrier carrier-name
color color
color-list list-name
domain-id domain-id
group-id group-id
omp-tag number
originator ip-address
preference number
```
Localized Control Policy Command Hierarchy

Configure on Cisco vEdge devices only.

```plaintext
policy
  lists
    as-path-list list-name
    as-path as-number
    community-list list-name
    community [aa:nn | internet | local-as | no-advertise | no-export]
    ext-community-list list-name
    community [rt (aa:nn | ip-address) | soo (aa:nn | ip-address)]
    prefix-list list-name
    ip-prefix prefix/length

policy
  route-policy policy-name
  default-action action
  sequence number
  match
    address list-name
    as-path list-name
    community list-name
    ext-community list-name
    local-preference number
    metric number
    next-hop list-name
    omp-tag number
    origin {egp | igp | incomplete}
    ospf-tag number
    peer address
  action
    reject
    accept
  set
    aggregator as-number ip-address
    as-path (exclude | prepend) as-number
    atomic-aggregate
    community value
    local-preference number
    metric number
    metric-type (type1 | type2)
    next-hop ip-address
    omp-tag number
    origin {egp | igp | incomplete}
    originator ip-address
```

ospf-tag number
weight number

vpn vpn-id
router
bgp local-as-number
  address-family ipv4-unicast
    redistribute (connected | nat | omp | ospf | static) [route-policy policy-name]
  neighbor address
    address-family ipv4-unicast
      route-policy policy-name (in | out)
ospf
  redistribute (bgp | connected | nat | omp | static) route-policy policy-name
  route-policy policy-name in

Centralized Data Policy Command Hierarchy

Configure on Cisco vSmart Controllers only.

centralized
policy
lists
  app-list list-name
    (app applications | app-family application-families)
  data-prefix-list list-name
  ip-prefix prefix/length
  site-list list-name
  site-id site-id
  tloc-list list-name
    tloc ip-address color color encap encapsulation [preference value weight value]
vpn-list list-name
  vpn vpn-id

centralized
policy
  data-policy policy-name
  vpn-list list-name
    default-action action
    sequence number
    match
      app-list list-name
      destination-data-prefix-list list-name
      destination-ip prefix/length
      destination-port number
      dns (request | response)
      dns-app-list list-name
      dscp number
      packet-length number
      plp (high | low)
      protocol number
      source-data-prefix-list list-name
      source-ip prefix/length
      source-port number
      tcp flag
    action
cflowd
    count counter-name
    drop
    log
tcp-optimization
    accept
      nat [pool number] [use-vpn-0]
      redirect-dns (host | ip-address)
    set
dscp number
    forwarding-class class
    local-tloc color color [encap encapsulation]
localized Data Policy Command Hierarchy

For IPv4

Configure on Cisco vEdge devices only.

cisco local-tloc-list color color [encap encapsulation] [restrict]
next-hop ip-address
policer policer-name
service service-name local [restrict] [vpn vpn-id]
service service-name [tloc ip-address | tloc-list list-name] [vpn vpn-id]
tloc ip-address color color [encap encapsulation]
tloc-list list-name
vpn vpn-id
vpn-membership policy-name
default-action action
sequence number
match
  vpn vpn-id
  vpn-list list-name
action
  (accept | reject)
apply-policy

site-list list-name data-policy policy-name (all | from-service | from-tunnel)
site-list list-name vpn-membership policy-name
source-ip prefix-length
source-port number
tcp flag
action
drop
count counter-name
log
accept
class class-name
count counter-name
log
mirror mirror-name
policer policer-name
set dscp value

vpn vpn-id
  interface interface-name
  access-list acl-name (in | out)

For IPv6

Configure on Cisco vEdge devices only.

policy ipv6
class-map
class class map map
mirror mirror-name
  remote-dest ip-address source ip-address
policer policer-name
  rate bandwidth
  burst bytes
  exceed action

policy ipv6
access-list list-name
sequence number
match
match-parameters
action
drop
count counter-name
log
accept
class class-name
  mirror mirror-name
  policer policer-name
default-action
  (accept | drop)

vpn vpn-id
  interface interface-name
  ipv6 access-list list-name (in | out)

Operational Commands

show running-config
Forward Error Correction

Forward Error Correction (FEC) is a mechanism to recover lost packets on a link by sending extra “parity” packets for every group (N) of packets. As long as the receiver receives a subset of packets in the group (at-least N-1) and the parity packet, up to a single lost packet in the group can be recovered. FEC is only supported on vEdge1000, 2000, and 5000 routers.

FEC adaptive only works when the app-route interval is set at least twice that of the BFD Hello packet interval.

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco SD-WAN 19.1</td>
<td>Feature introduced. Forward Error Correction (FEC) is a mechanism to recover lost packets on a link by sending extra “parity” packets for every group (N) of packets.</td>
</tr>
</tbody>
</table>

- Configure Forward Error Correction for a Policy, on page 157
- Monitor Forward Error Correction Tunnel Information, on page 158
- Monitor Forward Error Application Family Information, on page 159

Configure Forward Error Correction for a Policy

To configure FEC, follow these steps:

Step 1  Select Configuration > Policies.
Step 2  Select Centralized Policy.
Step 3  Select Centralized Policy at the top of the page and then click Add Policy.
Step 4  Click Next twice to select Configure Traffic Rules
Step 5  Select Traffic Data, and from the Add Policy drop-down menu select click Create New.
Step 6  Click Sequence Type in the left panel.
Step 7  From the Add Data Policy pop-up menu, select QoS.
Step 8  Click Sequence Rule.
Step 9  Click Applications/Application Family List/Data Prefix.
Step 10 Select one or more applications or lists.
Step 11 Click Actions and select Loss Correction.
Step 12 In the Actions area, select one of the following:
   • **FEC Adaptive**—Only send FEC information only when the system detects a packet loss.
     **Note** The FEC Adaptive option is supported only for Cisco vEdge devices.
   • **FEC Always**—Always send FEC information with every transmission
   • **Packet Duplication** check box—Duplicates packets through secondary links to reduce packet loss if one link goes down
Step 13 Click Save Match and Actions.
Step 14 Click Save Data Policy.
Step 15 Click Next and take these actions to create a Centralized Policy:
   a) Enter a Name and Description.
   b) Select Traffic Data Policy.
   c) Choose VPNs/site list for the policy.
   d) Save the policy.

**Monitor Forward Error Correction Tunnel Information**

To monitor FEC tunnel information, follow these steps:

Step 1  Select **Monitor > Network**.
Step 2  Select a device group.
Step 3  In the left panel, click **Tunnel**, which displays under WAN.

The WAN tunnel information includes the following:
   • A graph that shows the total tunnel loss for the selected tunnels.
   • A graph that shows the FEC loss recovery rate for the selected tunnels. The system calculates this rate by dividing the total number of reconstructed packets by the total number of lost packets on FEC:
   • A table that provides the following information for each tunnel endpoint:
     • Name of the tunnel endpoint
     • Communications protocol that the endpoint uses
     • State of the endpoint
     • Jitter, in ms, on the endpoint
     • Packet loss percentage for the endpoint
     • FEC loss recovery percentage for the endpoint
• Latency, in ms, on the endpoint
• Total bytes transmitted from the endpoint
• Total bytes received by the endpoint
• Application usage link

Monitor Forward Error Application Family Information

To monitor FEC application family information, follow these steps:

Step 1 Select Monitor &gt; Network.
Step 2 Select a device group.
Step 3 In the left panel, click DPI, which displays under WAN.

The FEC application information includes the following:

• A graph for which you can select any of the following perspectives:
  • Application Usage—Usage of various types of traffic for the selected application families, in KB.
  • Application Goodput—Goodput metadata for the selected application families.
  • Mean Opinion Score (MOS)—MOS for the selected application families.
  • FEC Recovery Rate—FEC loss recovery rate for the selected application families. The system calculates this rate by dividing the total number of reconstructed packets by the total number of lost FEC-enabled packets.

• A table that provides the following for each application family:
  • Name of the application family.
  • Goodput, in kbps, for the application family.
  • MOS for the selected application family.
  • FEC loss recovery percentage for the application family.
  • Traffic usage, in MB, for the selected application family.
Forward Error Correction

Monitor Forward Error Application Family Information
Packet Duplication for Noisy Channels

Table 22: Feature History

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco SD-WAN 19.2 and Cisco IOS XE SD-WAN 16.12</td>
<td>Feature introduced. This feature helps mitigate packet loss over noisy channels, thereby maintaining high application QoE for voice and video. This feature is supported on Cisco XE SD-WAN devices as well as on Cisco vEdge devices.</td>
</tr>
</tbody>
</table>

- Configure and Monitor Packet Duplication, on page 161

Configure and Monitor Packet Duplication

Cisco vEdge devices and Cisco XE SD-WAN devices use packet duplication to overcome packet loss. Packet duplication sends copies of packets on alternate available paths to reach Cisco vEdge devices and Cisco XE SD-WAN devices. If one of the packets is lost, a copy of the packet is forwarded to the server. Receiving Cisco vEdge devices and Cisco XE SD-WAN devices discard copies of the packet and forward one packet to the server.

Packet duplication is suitable for edges with multiple access links. Once packet duplication is configured and pushed to your device, you can see the tunnel packet duplication statistics.

Configure Packet Duplication

To configure packet duplication, follow these steps:

Step 1  Select Configuration > Policies.
Step 2  Select Centralized Policy.
Step 3  Select Centralized Policy at the top of the page and then click Add Policy.
Step 4  Click Next twice to select Configure Traffic Rules.
Step 5  Select Traffic Data, and from the Add Policy drop-down menu, select click Create New.
Step 6  Click Sequence Type in the left panel.
Step 7  From the Add Data Policy pop-up menu, select QoS.
Step 8  Click Sequence Rule.
Step 9 Click Applications/Application Family List/Data Prefix.
Step 10 Select one or more applications or lists.
Step 11 Click Actions and select Loss Correction.
Step 12 In the Actions area, select the Pack Duplication option to enable the packet duplication feature.
  - FEC Adaptive—Only send Forward Error Correction (FEC) information when the system detects a packet loss.
  - FEC Always—Always send FEC information with every transmission.
  - None—Use when no loss protection is needed.
  - Packet Duplication—Enable when packets need to be duplicated and sent on the next available links to reduce packet loss.
Step 13 Click Save Match and Actions.
Step 14 Click Save Data Policy.
Step 15 Click Next and take these actions to create a Centralized Policy:
  - Enter a Name and a Description.
  - Select Traffic Data Policy.
  - Choose VPNs/site list for the policy.
  - Save the policy.

Monitor Packet Duplication Per Application

To monitor packet duplication enabled per application, follow these steps:

Step 1 Select Monitor > Network.
Step 2 Select a device group.
Step 3 In the left panel, click Applications.
Step 4 On the Application usage tab, select the application family of interest, and click on the Application family listed.
Step 5 If packet duplication is enabled for any application, vManage displays Packet Delivery Performance as GOOD, MODERATE, or POOR or the field displays as N/A.
Step 6 GOOD and MODERATE performance is a clickable link. When clicking on the link, the status pops up a window.
Step 7 On the pop-up window, you see Application, Packet Delivery Performance, Overall for the Application, Average Drop Rate, and Overall for the Application information. The time slot graph represents the packets transmitted with different available link colors and the overall performance calculated when packet duplication is enabled.
Step 8 If you hover over the time slot, you can see the performance status and the average drop rate for each link.
Application-Aware Routing

Application-aware routing tracks network and path characteristics of the data plane tunnels between Cisco devices and uses the collected information to compute optimal paths for data traffic. These characteristics include packet loss, latency, and jitter, and the load, cost and bandwidth of a link. The ability to consider factors in path selection other than those used by standard routing protocols—such as route prefixes, metrics, link-state information, and route removal on the Cisco device—offers a number of advantages to an enterprise:

• In normal network operation, the path taken by application data traffic through the network can be optimized, by directing it to WAN links that support the required levels of packet loss, latency, and jitter defined in an application’s SLA.

• In the face of network brownouts or soft failures, performance degradation can be minimized. The tracking of network and path conditions by application-aware routing in real time can quickly reveal performance issues, and it automatically activates strategies that redirect data traffic to the best available path. As the network recovers from the brownout or soft failure conditions, application-aware routing automatically readjusts the data traffic paths.

• Network costs can be reduced because data traffic can be more efficiently load-balanced.

• Application performance can be increased without the need for WAN upgrades.
Each Cisco device supports up to eight TLOCs, allowing a single Cisco device to connect to up to eight different WAN networks. This capability allows path customization for application traffic that has different needs in terms of packet loss and latency.

- Components of Application-Aware Routing, on page 164
- Classification of Tunnels into SLA Classes, on page 165
- Configure Application-Aware Routing, on page 167
- Configure Application Aware Routing Using CLIs, on page 175
- Structural Components of Policy Configuration for Application-Aware Routing, on page 177
- Apply Application-Aware Routing Policy, on page 184
- Configure the Monitoring of Data Plane Tunnel Performance, on page 186
- Application-Aware Routing Policy Configuration Example, on page 187

**Components of Application-Aware Routing**

The Cisco SD-WAN Application-Aware Routing solution consists of three elements:

- **Identification**—You define the application of interest, and then you create a centralized data policy that maps the application to specific SLA requirements. You single out data traffic of interest by matching on the Layer 3 and Layer 4 headers in the packets, including source and destination prefixes and ports, protocol, and DSCP field. As with all centralized data policies, you configure them on a Cisco vSmart Controller, which then passes them to the appropriate Cisco devices.

- **Monitoring and measuring**—The Cisco SD-WAN software uses BFD packets to continuously monitor the data traffic on the data plane tunnels between Cisco devices, and periodically measures the performance characteristics of the tunnel. To gauge performance, the Cisco SD-WAN software looks for traffic loss...
on the tunnel, and it measures latency by looking at the one-way and round-trip times of traffic traveling over the tunnel. These measurements might indicate a blackout or brownout condition.

• **Mapping application traffic to a specific transport tunnel**—The final step is to map an application’s data traffic to the data plane tunnel that provides the desired performance for the application. The mapping decision is based on two criteria: the best-path criteria computed from measurements performed on the WAN connections and on the constraints specified in a policy specific to application-aware routing.

To create data policy based on the Layer 7 application itself, use configure deep packet inspection with a centralized data policy. With deep packet inspection, you can direct traffic to a specific tunnel, based on the remote TLOC, the remote TLOC, or both. You cannot direct traffic to tunnels based on SLA classes.

## Classification of Tunnels into SLA Classes

The process of classifying tunnels into one or more SLA classes for application-aware routing has three parts:

- Measure loss, latency, and jitter information for the tunnel.
- Calculate the average loss, latency, and jitter for the tunnel.
- Determine the SLA classification of the tunnel.

### Measure Loss, Latency, and Jitter

When a data plane tunnel in the overlay network is established, a BFD session automatically starts on the tunnel. In the overlay network, each tunnel is identified with a color that identifies a specific link between a local TLOC and a remote TLOC. The BFD session monitors the liveness of the tunnel by periodically sending Hello packets to detect whether the link is operational. Application-aware routing uses the BFD Hello packets to measure the loss, latency, and jitter on the links.
By default, the BFD Hello packet interval is 1 second. This interval is user-configurable (with the `bfd color interval` command). Note that the BFD Hello packet interval is configurable per tunnel.

**Calculate Average Loss, Latency, and Jitter**

BFD periodically polls all the tunnels on the Cisco devices to collect packet latency, loss, jitter, and other statistics for use by application-aware routing. At each poll interval, application-aware routing calculates the average loss, latency, and jitter for each tunnel, and then calculates or recalculates each tunnel's SLA. Each poll interval is also called a "bucket."

By default, the poll interval is 10 minutes. With the default BFD Hello packet interval at 1 second, this means that information from about 600 BFD Hello packets is used in one poll interval to calculate loss, latency, and jitter for the tunnel. The poll interval is user-configurable (with the `bfd app-route poll-interval` command). Note that the application-aware routing poll interval is configurable per Cisco device; that is, it applies to all tunnels originating on a device.

Reducing the poll interval without reducing the BFD Hello packet interval may affect the quality of the loss, latency, and jitter calculation. For example, setting the poll interval to 10 seconds when the BFD Hello packet interval is 1 second means that only 10 Hello packets are used to calculate the loss, latency, and jitter for the tunnel.

The loss, latency, and jitter information from each poll interval is preserved for six poll intervals. At the seventh poll interval, the information from the earliest polling interval is discarded to make way for the latest information. In this way, application-aware routing maintains a sliding window of tunnel loss, latency, and jitter information.

The number of poll intervals (6) is not user-configurable. Each poll interval is identified by an index number (0 through 5) in the output of the `show app-route statistics` command.

**Determine the SLA Classification**

To determine the SLA classification of a tunnel, application-aware routing uses the loss, latency, and jitter information from the latest poll intervals. The number of poll intervals used is determined by a multiplier. By default, the multiplier is 6, so the information from all the poll intervals (specifically, from the last six poll intervals) is used to determine the classification. For the default poll interval of 10 minutes and the default multiplier of 6, the loss, latency, and jitter information collected over the last hour is considered when classifying the SLA of each tunnel. These default values have to be chosen to provide damping of sorts, as a way to prevent frequent reclassification (flapping) of the tunnel.

The multiplier is user-configurable (with the `bfd app-route multiplier` command). Note that the application-aware routing multiplier is configurable per Cisco device; that is, it applies to all tunnels originating on a device.

If there is a need to react quickly to changes in tunnel characteristics, you can reduce the multiplier all the way down to 1. With a multiplier of 1, only the latest poll interval loss and latency values are used to determine whether this tunnel can satisfy one or more SLA criteria.

Based on the measurement and calculation of tunnel loss and latency, each tunnel may satisfy one or more user-configured SLA classes. For example, a tunnel with a mean loss of 0 packets and mean latency of 10 milliseconds would satisfy a class that has been defined with a maximum packet loss of 5 and a minimum latency of 20 milliseconds, and it would also satisfy a class that has been defined with a maximum packet loss of 0 and minimum latency of 15 milliseconds.

Regardless of how quickly a tunnel is reclassified, the loss, latency, and jitter information is measured and calculated continuously. You can configure how quickly application-aware routing reacts to changes by modifying the poll interval and multiplier.
Configure Application-Aware Routing

This topic provides general procedures for configuring application-aware routing. Application-aware routing policy affects only traffic that is flowing from the service side (the local/WAN side) to the tunnel (WAN) side of the Cisco device.

An application-aware routing policy matches applications with an SLA, that is, with the data plane tunnel performance characteristics that are necessary to transmit the applications' data traffic. The primary purpose of application-aware routing policy is to optimize the path for data traffic being transmitted by Cisco devices.

An application-aware routing policy is a type of centralized data policy: you configure it on the Cisco vSmart Controller, and the controller automatically pushes it to the affected Cisco devices. As with any policy, an application-aware routing policy consists of a series of numbered (ordered) sequences of match-action pairs that are evaluated in order, from lowest sequence number to highest sequence number. When a data packet matches one of the match conditions, an SLA action is applied to the packet to determine the data plane tunnel to use to transmit the packet. If a packet matches no parameters in any of the policy sequences, and if no default SLA class is configured, the packet is accepted and forwarded with no consideration of SLA. Because application-aware routing policy accepts nonmatching traffic by default, it is considered to be a positive policy. Other types of policies in the Cisco SD-WAN software are negative policies, because by default they drop nonmatching traffic.

General Cisco vManage Configuration Procedure

To configure application-aware routing policy, use the Cisco vManage policy configuration wizard. The wizard consists of four sequential screens that guide you through the process of creating and editing policy components:

- Create Applications or Groups of Interest—Create lists that group together related items and that you call in the match or action components of a policy.
- Configure Topology—Create the network structure to which the policy applies.
- Configure Traffic Rules—Create the match and action conditions of a policy.
- Apply Policies to Sites and VPNs—Associate policy with sites and VPNs in the overlay network.

In the first three policy configuration wizard screens, you are creating policy components or blocks. In the last screen, you are applying policy blocks to sites and VPNs in the overlay network.

For an application-aware routing policy to take effect, you must activate the policy.

Step 1: Start the Policy Configuration Wizard

To start the policy configuration wizard:

1. In the Cisco vManage NMS, select the Configure > Policies screen. When you first open this screen, the Centralized Policy tab is selected by default.
2. Click Add Policy.

The policy configuration wizard opens, and the Create Applications or Groups of Interest screen is displayed.
Step 2: Create Applications or Groups of Interest

To create lists of applications or groups to use in centralized policy:

1. Create new lists of groups, as described in the following table:

   **Table 23:**

<table>
<thead>
<tr>
<th>List Type</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| Application | a. In the left bar, click **Application**.  
  b. Click **New Application List**.  
  c. Enter a name for the list.  
  d. Click either the **Application** or **Application Family** button.  
  e. From the Select drop-down, select the desired applications or application families.  
  f. Click **Add**.  

   Two application lists are preconfigured. You cannot edit or delete these lists.  
   • Google_Apps—Includes Google applications, such as gmail, Google maps, and YouTube. To display a full list of Google applications, click the list in the **Entries** column.  
   • Microsoft_Apps—Includes Microsoft applications, such as Excel, Skype, and Xbox. To display a full list of Microsoft applications, click the list in the **Entries** column.  

| Prefix | a. In the left bar, click **Prefix**.  
  b. Click **New Prefix List**.  
  c. Enter a name for the list.  
  d. In the Add Prefix field, enter one or more data prefixes separated by commas.  
  e. Click **Add**.  

| Site | a. In the left bar, click **Site**.  
  b. Click **New Site List**.  
  c. Enter a name for the list.  
  d. In the Add Site field, enter one or more site IDs separated by commas.  
  e. Click **Add**.  

### List Type | Procedure
--- | ---
**SLA Class**
a. In the left bar, click **SLA Class**.
b. Click **New SLA Class List**.
c. Enter a name for the list.
d. Define the SLA class parameters:
   1. In the **Loss** field, enter the maximum packet loss on the connection, a value from 0 through 100 percent.
   2. In the **Latency** field, enter the maximum packet latency on the connection, a value from 0 through 1,000 milliseconds.
   3. In the **Jitter** field, enter the maximum jitter on the connection, a value from 1 through 1,000 milliseconds.
e. Click **Add**.

**VPN**
a. In the left bar, click **VPN**.
b. Click **New VPN List**.
c. Enter a name for the list.
d. In the **Add VPN** field, enter one or more VPN IDs separated by commas.
e. Click **Add**.

2. Click **Next** to move to Configure Topology in the wizard. When you first open this screen, the Topology tab is selected by default.

**Step 3: Configure the Network Topology**

To configure the network topology:

1. In the Topology tab, create a network topology, as described in the following table:
Table 24:

<table>
<thead>
<tr>
<th>Policy Type</th>
<th>Description</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| Hub and Spoke | Policy for a topology with one or more central hub sites and with spokes connected to a hub | a. In the Add Topology drop-down, select **Hub and Spoke**.  
b. Enter a name for the hub-and-spoke policy.  
c. Enter a description for the policy.  
d. In the VPN List field, select the VPN list for the policy.  
e. In the left pane, click **Add Hub and Spoke**. A hub-and-spoke policy component containing the text string My Hub-and-Spoke is added in the left pane.  
f. Double-click the **My Hub-and-Spoke** text string, and enter a name for the policy component.  
g. In the right pane, add hub sites to the network topology:  
   1. Click **Add Hub Sites**.  
   2. In the Site List Field, select a site list for the policy component.  
   3. Click **Add**.  
   4. Repeat Steps 7a, 7b, and 7c to add more hub sites to the policy component.  

h. In the right pane, add spoke sites to the network topology:  
   1. Click **Add Spoke Sites**.  
   2. In the Site List Field, select a site list for the policy component.  
   3. Click **Add**.  
   4. Repeat Steps 8a, 8b, and 8c to add more spoke sites to the policy component.  
i. Repeat Steps 5 through 8 to add more components to the hub-and-spoke policy.  
j. Click **Save Hub and Spoke Policy**.
### Procedure Description

<table>
<thead>
<tr>
<th>Policy Type</th>
<th>Description</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mesh</td>
<td>Partial-mesh or full-mesh region</td>
<td>a.  In the Add Topology drop-down, select <strong>Mesh</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>b.  Enter a name for the mesh region policy component.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>c.  Enter a description for the mesh region policy component.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>d.  In the VPN List field, select the VPN list for the policy.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>e.  Click <strong>New Mesh Region</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>f.  In the Mesh Region Name field, enter a name for the individual mesh region.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>g.  In the Site List field, select one or more sites to include in the mesh region.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>h.  Repeat Steps 5 through 7 to add more mesh regions to the policy.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>i.  Click <strong>Save Mesh Region</strong>.</td>
</tr>
</tbody>
</table>

2. To use an existing topology:
   a.  In the Add Topology drop-down, click **Import Existing Topology**. The Import Existing Topology popup displays.
   b.  Select the type of topology.
   c.  In the Policy drop-down, select the name of the topology.
   d.  Click **Import**.

3. Click **Next** to move to Configure Traffic Rules in the wizard. When you first open this screen, the Application-Aware Routing tab is selected by default.

### Step 4: Configure Traffic Rules

To configure traffic rules for application-aware routing policy:

1. In the Application-Aware Routing bar, select the **Application-Aware Routing** tab.
2. Click the **Add Policy** drop-down.
3. Select **Create New**, and in the left pane, click **Sequence Type**. A policy sequence containing the text string App Route is added in the left pane.
4. Double-click the App Route text string, and enter a name for the policy sequence. The name you type is displayed both in the Sequence Type list in the left pane and in the right pane.
5. In the right pane, click **Sequence Rule**. The Match/Action box opens, and Match is selected by default. The available policy match conditions are listed below the box.
6. To select one or more Match conditions, click its box and set the values as described in the following table:
Table 25:

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>None (match all packets)</td>
<td>Do not specify any match conditions.</td>
</tr>
<tr>
<td>Applications/Application Family List</td>
<td>In the Match conditions, click Applications/Application Family List.</td>
</tr>
<tr>
<td></td>
<td>b. In the drop-down, select the application family.</td>
</tr>
<tr>
<td></td>
<td>c. To create an application list:</td>
</tr>
<tr>
<td></td>
<td>1. Click <strong>New Application List</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. Enter a name for the list.</td>
</tr>
<tr>
<td></td>
<td>3. Click the <strong>Application</strong> button to create a list of individual applications. Click the <strong>Application Family</strong> button to create a list of related applications.</td>
</tr>
<tr>
<td></td>
<td>4. In the Select Application drop-down, select the desired applications or application families.</td>
</tr>
<tr>
<td></td>
<td>5. Click <strong>Save</strong>.</td>
</tr>
<tr>
<td>Destination Data Prefix</td>
<td>a. In the Match conditions, click Destination Data Prefix.</td>
</tr>
<tr>
<td></td>
<td>b. To match a list of destination prefixes, select the list from the drop-down.</td>
</tr>
<tr>
<td></td>
<td>c. To match an individual destination prefix, type the prefix in the Destination box.</td>
</tr>
<tr>
<td>Destination Port</td>
<td>a. In the Match conditions, click Destination Port.</td>
</tr>
<tr>
<td></td>
<td>b. In the Destination field, enter the port number. Specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]).</td>
</tr>
<tr>
<td>DNS Application List (to enable split DNS)</td>
<td>a. In the Match conditions, click DNS Application List.</td>
</tr>
<tr>
<td></td>
<td>b. In the drop-down, select the application family.</td>
</tr>
<tr>
<td>DNS (to enable split DNS)</td>
<td>a. In the Match conditions, click DNS.</td>
</tr>
<tr>
<td></td>
<td>b. In the drop-down, select Request to process DNS requests for the DNS applications, and select Response to process DNS responses for the applications.</td>
</tr>
<tr>
<td>DSCP</td>
<td>a. In the Match conditions, click DSCP.</td>
</tr>
<tr>
<td></td>
<td>b. In the DSCP field, type the DSCP value, a number from 0 through 63.</td>
</tr>
</tbody>
</table>
a. In the Match conditions, click **PLP**.
b. In the PLP drop-down, select **Low** or **High**. To set the PLP to high, apply a policer that includes the **exceed remark** option.

**Protocol**

a. In the Match conditions, click **Protocol**.
b. In the Protocol field, type the Internet Protocol number, a number from 0 through 255.

**Source Data Prefix**

a. In the Match conditions, click **Source Data Prefix**.
b. To match a list of source prefixes, select the list from the drop-down.
c. To match an individual source prefix, type the prefix in the Source box.

**Source Port**

a. In the Match conditions, click **Source Port**.
b. In the Source field, enter the port number. Specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]).

7. To select actions to take on matching data traffic, click the **Actions** box. The available policy actions are listed below the box.

8. Set the policy action as described in the following table:

   **Table 26:**

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Description</th>
<th>Procedure</th>
</tr>
</thead>
</table>
   | **Backup SLA Preferred Color**   | When no tunnel matches the SLA, direct the data traffic to a specific tunnel. Data traffic is sent out the configured tunnel if that tunnel interface is available. If that tunnel interface is not available, traffic is sent out another available tunnel. You can specify one or more colors. The backup SLA preferred color is a loose matching, not a strict matching. | a. In the Action conditions, click **Backup SLA Preferred Color**.  
b. In the drop-down, select one or more colors. |
   | **Counter**                      | Count matching data packets.                                               | a. In the Action conditions, click **Counter**.  
b. In the Counter Name field, enter the name of the file in which to store packet counters. |
**Log**

Place a sampled set of packets that match the SLA class rule into system logging (syslog) files. In addition to logging the packet headers, a syslog message is generated the first time a packet header is logged and then every 5 minutes thereafter, as long as the flow is active.

<table>
<thead>
<tr>
<th>Log</th>
<th>Place a sampled set of packets that match the SLA class rule into system logging (syslog) files. In addition to logging the packet headers, a syslog message is generated the first time a packet header is logged and then every 5 minutes thereafter, as long as the flow is active.</th>
</tr>
</thead>
</table>

**SLA Class List**

For the SLA class, all matching data traffic is directed to a tunnel whose performance matches the SLA parameters defined in the class. The software first tries to send the traffic through a tunnel that matches the SLA. If a single tunnel matches the SLA, data traffic is sent through that tunnel. If two or more tunnels match, traffic is distributed among them. If no tunnel matches the SLA, data traffic is sent through one of the available tunnels.

<table>
<thead>
<tr>
<th>SLA Class List</th>
<th>For the SLA class, all matching data traffic is directed to a tunnel whose performance matches the SLA parameters defined in the class. The software first tries to send the traffic through a tunnel that matches the SLA. If a single tunnel matches the SLA, data traffic is sent through that tunnel. If two or more tunnels match, traffic is distributed among them. If no tunnel matches the SLA, data traffic is sent through one of the available tunnels.</th>
</tr>
</thead>
</table>

**Step 5: Apply Policies to Sites and VPNs**

In the last screen of the policy configuration wizard, you associate the policy blocks that you created on the previous three screens with VPNs and with sites in the overlay network.

To apply a policy block to sites and VPNs in the overlay network:

1. If you are already in the policy configuration wizard, skip to Step 6. Otherwise, in the Cisco vManage NMS, select the **Configure > Policies** screen. When you first open this screen, the Centralized Policy tab is selected by default.

2. Click **Add Policy**. The policy configuration wizard opens, and the Create Applications or Groups of Interest screen is displayed.

3. Click **Next**. The Network Topology screen opens, and in the Topology bar, the Topology tab is selected by default.
Configure Application Aware Routing Using CLIs

Following are the high-level steps for configuring an application-aware routing policy:

1. Create a list of overlay network sites to which the application-aware routing policy is to be applied (in the `apply-policy` command):

   ```
   vSmart(config)# policy
   vSmart(config-policy)# lists site-list list-name
   vSmart(config-site-list)# site-id site-id
   ```

   The list can contain as many site IDs as necessary. Include one `site-id` command for each site ID. For contiguous site IDs, you can specify a range of numbers separated with a dash (–). Create additional site lists, as needed.

2. Create SLA classes and traffic characteristics to apply to matching application data traffic:

   ```
   vSmart(config)# policy sla-class sla-class-name
   vSmart(config-sla-class)# jitter milliseconds
   ```
Configure Application Aware Routing

Using CLIs

vSmart(config-sla-class)# latency milliseconds
vSmart(config-sla-class)# loss percentage

3. Create lists of applications, IP prefixes, and VPNs to use in identifying application traffic of interest (in the **match** section of the policy definition):

vSmart(config)# policy lists
vSmart(config-lists)# app-list list-name
vSmart(config-app-list)# (app application-name | app-family family-name)

vSmart(config-lists)# prefix-list list-name
vSmart(config-prefix-list)# ip-prefix prefix/length

vSmart(config-lists)# vpn-list list-name
vSmart(config-vpn-list)# vpn vpn-id

4. If you are configuring a logging action, configure how often to log packets to syslog files:

vEdge(config)# policy log-frequency number

5. Create an application-aware routing policy instance and associate it with a list of VPNs:

vSmart(config)# policy app-route-policy policy-name
vSmart(config-app-route-policy)# vpn-list list-name

6. Within the policy, create one or more numbered sequence of match–action pairs, where the match parameters define the data traffic and applications of interest and the action parameters specify the SLA class to apply if a match occurs.

a. Create a sequence:

vSmart(config-app-route-policy)# sequence number

b. Define match parameters for data packets:

vSmart(config-sequence)# match parameters

c. Define the action to take if a match occurs:

vSmart(config-sequence)# action sla-class sla-class-name [strict]
vSmart(config-sequence)# action sla-class sla-class-name [strict] preferred-color colors
vSmart(config-sequence)# action backup-sla-preferred-color colors

The first two **action** options direct matching data traffic to a tunnel interface that meets the SLA characteristics in the specified SLA class:

- **sla-class sla-class-name**—When you specify an SLA class with no additional parameters, data traffic that matches the SLA is forwarded as long as one tunnel interface is available. The software first tries to send the traffic through a tunnel that matches the SLA. If a single tunnel matches the SLA, data traffic is sent through that tunnel. If two or more tunnels match, traffic is distributed among them. If no tunnel matches the SLA, data traffic is sent through one of the available tunnels.

- **sla-class sla-class-name preferred-color color**—To set a specific tunnel to use when data traffic matches an SLA class, include the **preferred-color** option, specifying the color of the preferred tunnel. If more than one tunnel matches the SLA, traffic is sent to the preferred tunnel. If a tunnel of the preferred color is not available, traffic is sent through any tunnel that matches the SLA class. If no tunnel matches the SLA, data traffic is sent through any available tunnel. In this sense, color preference is considered to be a loose matching, not a strict matching, because data traffic is always forwarded, whether a tunnel of the preferred color is available or not.
- **sla-class sla-class-name preferred-color colors**—To set multiple tunnels to use when data traffic matches an SLA class, include the `preferred-color` option, specifying two or more tunnel colors. Traffic is load-balanced across all tunnels.

If no tunnel matches the SLA, data traffic is sent through any available tunnel. In this sense, color preference is considered to be a loose matching, not a strict matching, because data traffic is always forwarded, whether a tunnel of the preferred color is available or not. When no tunnel matches the SLA, you can choose how to handle the data traffic:

- **strict**—Drop the data traffic.
- **backup-sla-preferred-color colors**—Direct the data traffic to a specific tunnel. Data traffic is sent out the configured tunnel if that tunnel interface is available; if that tunnel is unavailable, traffic is sent out another available tunnel. You can specify one or more colors. As with the `preferred-color` option, the backup SLA preferred color is loose matching. In a single `action` configuration, you cannot include both the `strict` and `backup-sla-preferred-color` options.

d. Count the packets or bytes that match the policy:
   ```
   vSmart(config-sequence)# action count counter-name
   ```
e. Place a sampled set of packets that match the SLA class rule into syslog files:
   ```
   vSmart(config-sequence)# action log
   ```
f. The match–action pairs within a policy are evaluated in numerical order, based on the sequence number, starting with the lowest number. If a match occurs, the corresponding action is taken and policy evaluation stops.

7. If a packet does not match any of the conditions in one of the sequences, a default action is taken. For application-aware routing policy, the default action is to accept nonmatching traffic and forward it with no consideration of SLA. You can configure the default action so that SLA parameters are applied to nonmatching packets:
   ```
   vSmart(config-policy-name)# default-action sla-class sla-class-name
   ```

8. Apply the policy to a site list:
   ```
   vSmart(config)# apply-policy site-list list-name app-route-policy policy-name
   ```

### Structural Components of Policy Configuration for Application-Aware Routing

Here are the structural components required to configure application-aware routing policy. Each one is explained in more detail in the sections below.

```python
policy
 lists
   app-list list-name
     (app application-name | app-family application-family)
   prefix-list list-name
   ip-prefix prefix
   site-list list-name
   site-id site-id
   vpn-list list-name
```
Lists

Application-aware routing policy uses the following types of lists to group related items. You configure these lists under the **policy lists** command hierarchy on Cisco vSmart Controllers.
Table 27:

<table>
<thead>
<tr>
<th>List Type</th>
<th>Description</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications and application families</td>
<td>List of one or more applications or application families running on the subnets connected to the Cisco device. Each app-list can contain either applications or application families, but you cannot mix the two. To configure multiple applications or application families in a single list, include multiple app or app-family options, specifying one application or application family in each app or app-family option.</td>
<td>`app-list list-name (app application-name</td>
</tr>
<tr>
<td></td>
<td>• application-name is the name of an application. The Cisco SD-WAN software supports about 2300 different applications.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• application-family is the name of an application family. It can one of the following: antivirus, application-service, audio_video, authentication, behavioral, compression, database, encrypted, erp, file-server, file-transfer, forum, game, instant-messaging, mail, microsoft-office, middleware, network-management, network-service, peer-to-peer, printer, routing, security-service, standard, telephony, terminal, thin-client, tunneling, wap, web, and webmail.</td>
<td></td>
</tr>
<tr>
<td>Data prefixes</td>
<td>List of one or more IP prefixes. To configure multiple prefixes in a single list, include multiple ip-prefix options, specifying one prefix in each option.</td>
<td><code>data-prefix-list list-name ip-prefix prefix/length</code></td>
</tr>
<tr>
<td>List Type</td>
<td>Description</td>
<td>Command</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>---------</td>
</tr>
<tr>
<td>Sites</td>
<td>List of one or more site identifiers in the overlay network. To configure multiple sites in a single list, include multiple <code>site-id</code> options, specifying one site number in each option. You can specify a single site identifier (such as <code>site-id 1</code>) or a range of site identifiers (such as <code>site-id 1-10</code>).</td>
<td><code>site-list list-name site-id site-id</code></td>
</tr>
<tr>
<td>VPNs</td>
<td>List of one or more VPNs in the overlay network. To configure multiple VPNs in a single list, include multiple <code>vpn</code> options, specifying one VPN number in each option. You can specify a single VPN identifier (such as <code>vpn-id 1</code>) or a range of VPN identifiers (such as <code>vpn-id 1-10</code>).</td>
<td><code>vpn-list list-name vpn vpn-id</code></td>
</tr>
</tbody>
</table>

In the Cisco vSmart Controller configuration, you can create multiple iterations of each type of list. For example, it is common to create multiple site lists and multiple VPN lists so that you can apply data policy to different sites and different customer VPNs across the network.

When you create multiple iterations of a type of list (for example, when you create multiple VPN lists), you can include the same values or overlapping values in more than one of these lists. You can do this either on purpose, to meet the design needs of your network, or you can do this accidentally, which might occur when you use ranges to specify values. (You can use ranges to specify data prefixes, site identifiers, and VPNs.) Here are two examples of lists that are configured with ranges and that contain overlapping values:

- `vpn-list list-1 vpn 1-10`
  `vpn-list list-2 vpn 6-8`
- `site-list list-1 site 1-10`
  `site-list list-2 site 5-15`

When you configure data policies that contain lists with overlapping values, or when you apply data policies, you must ensure that the lists included in the policies, or included when applying the policies, do not contain overlapping values. To do this, you must manually audit your configurations. The Cisco SD-WAN configuration software performs no validation on the contents of lists, on the data policies themselves, or on how the policies are applied to ensure that there are no overlapping values.

If you configure or apply data policies that contain lists with overlapping values to the same site, one policy is applied and the others are ignored. Which policy is applied is a function of the internal behavior of Cisco SD-WAN software when it processes the configuration. This decision is not under user control, so the outcome is not predictable.

**Logging Frequency**

If you configure a logging action, by default, the Cisco vEdge device logs all data packet headers to a syslog file. To log only a sample of the data packet headers:

```
vEdge(config)# policy log-frequency number
```
number specifies how often to log packet headers. For example, if you configure log-frequency 20, every sixteenth packet is logged. While you can configure any integer value for the frequency, the software rounds the value down to the nearest power of 2.

SLA Classes

The action taken in application-aware routing is applied based on what is called an SLA (a service-level agreement). An SLA class is defined by the maximum jitter, maximum latency, maximum packet loss, or a combination of these values, for the Cisco device's data plane tunnels. (Each tunnel is defined by a local TLOC–remote TLOC pair.) You configure SLA classes under the policy sla-class command hierarchy on Cisco vSmart Controllers. You can configure a maximum of four SLA classes.

You can configure the following parameters in an SLA class:

<table>
<thead>
<tr>
<th>Description</th>
<th>Command</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum acceptable packet jitter on the data plane tunnel</td>
<td>jitter milliseconds</td>
<td>1 through 1000 milliseconds</td>
</tr>
<tr>
<td>Maximum acceptable packet latency on the data plane tunnel</td>
<td>latency milliseconds</td>
<td>1 through 1000 milliseconds</td>
</tr>
<tr>
<td>Maximum acceptable packet loss on the data plane tunnel</td>
<td>loss percentage</td>
<td>0 through 100 percent</td>
</tr>
</tbody>
</table>

VPN Lists

Each application-aware policy instance is associated with a VPN list. You configure VPN lists with the policy app-route-policy vpn-list command. The VPN list you specify must be one that you created with a policy lists vpn-list command.

Sequences

Within each VPN list, an application-aware policy contains sequences of match–action pairs. The sequences are numbered to set the order in which data traffic is analyzed by the match–action pairs in the policy. You configure sequences with the policy app-aware-policy vpn-list sequence command.

Each sequence in an application-aware policy can contain one match command and one action command.

Match Parameters

Application-aware routing policy can match IP prefixes and fields in the IP headers. You configure the match parameters with the match command under the policy app-route-policy vpn-list sequence command hierarchy on Cisco vSmart Controllers.

You can match these parameters:

<table>
<thead>
<tr>
<th>Description</th>
<th>Command</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Match all packets</td>
<td>Omit match command</td>
<td>——</td>
</tr>
<tr>
<td>Description</td>
<td>Command</td>
<td>Value or Range</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>--------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Applications or application families</td>
<td>app-list list-name</td>
<td>Name of an app-list list</td>
</tr>
<tr>
<td>Group of destination prefixes</td>
<td>destination-data-prefix-list</td>
<td>Name of a data-prefix-list list</td>
</tr>
<tr>
<td>Individual destination prefix</td>
<td>destination-ip prefix/length</td>
<td>IP prefix and prefix length</td>
</tr>
<tr>
<td>Destination port number</td>
<td>destination-port number</td>
<td>0 through 65535. Specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]).</td>
</tr>
<tr>
<td>DSCP value</td>
<td>dscp number</td>
<td>0 through 63</td>
</tr>
<tr>
<td>Internet Protocol number</td>
<td>protocol number</td>
<td>0 through 255</td>
</tr>
<tr>
<td>Packet loss priority (PLP)</td>
<td>plp</td>
<td>(high</td>
</tr>
<tr>
<td>Group of source prefixes</td>
<td>source-data-prefix-list list-name</td>
<td>Name of a data-prefix-list list</td>
</tr>
<tr>
<td>Individual source prefix</td>
<td>source-ip prefix/length</td>
<td>IP prefix and prefix length</td>
</tr>
<tr>
<td>Source port number</td>
<td>source-port number</td>
<td>0 through 65535; enter a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]).</td>
</tr>
<tr>
<td>Split DNS, to resolve and process DNS requests on an application-by-application basis</td>
<td>dns-app-list list-name</td>
<td>Name of an app-list list. This list specifies the applications whose DNS requests are processed.</td>
</tr>
<tr>
<td></td>
<td>dns (request</td>
<td>response)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To process DNS responses returned from DNS servers to the applications, specify dns response.</td>
</tr>
</tbody>
</table>

**Action Parameters**

When data traffic matches the match parameters, the specified action is applied to it. For application-aware routing policy, the action is to apply an SLA class. The SLA class defines the maximum packet latency or maximum packet loss, or both, that the application allows on the data plane tunnel used to transmit its data.
The Cisco SD-WAN software examines the recently measured performance characteristics of the data plane tunnels and directs the data traffic to the WAN connection that meets the specified SLA.

The following actions can be configured:

**Table 30:**

<table>
<thead>
<tr>
<th>Description</th>
<th>Command</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>When no tunnel matches the SLA, direct the data traffic to a specific tunnel. Data traffic is sent out the configured tunnel if that tunnel interface is available. If that tunnel is unavailable, traffic is sent out another available tunnel. You can specify one or more colors. The backup SLA preferred color is a loose matching, not a strict matching.</td>
<td>backup-sla-preferred-color colors</td>
<td>3g, biz-internet, blue, bronze, custom1, custom2, custom3, default, gold, green lte, metro-ethernet, mpls, private1 through private6, public-internet, red, silver</td>
</tr>
<tr>
<td>Count matching data packets.</td>
<td>action count counter-name</td>
<td>Name of a counter.</td>
</tr>
<tr>
<td>Place a sampled set of packets that match the SLA class rule into the messages and vsyslog system logging (syslog) files. In addition to logging the packet headers, a syslog message is generated the first time a packet header is logged and then every 5 minutes thereafter, as long as the flow is active.</td>
<td>action log</td>
<td>To display logging information, use the show app log flow-all, show app log flows, and show log commands on the Cisco vEdge device.</td>
</tr>
<tr>
<td>SLA class to match. All matching data traffic is directed to a tunnel whose performance matches the SLA parameters defined in the class. The software first tries to send the traffic through a tunnel that matches the SLA. If a single tunnel matches the SLA, data traffic is sent through that tunnel. If two or more tunnels match, traffic is distributed among them. If no tunnel matches the SLA, data traffic is sent through one of the available tunnels.</td>
<td>action sla-class sla-class-name</td>
<td>SLA class name defined in policy sla-class command</td>
</tr>
<tr>
<td>Group of data plane tunnel colors to prefer when an SLA class match occurs. Traffic is load-balanced across all tunnels. If no tunnels match the SLA, data traffic is sent through any available tunnel. That is, color preference is a loose matching, not a strict matching.</td>
<td>action sla-class sla-class-name preferred-color colors</td>
<td>SLA class name defined in policy sla-class command and one of the supported tunnel colors.</td>
</tr>
</tbody>
</table>
### Description

Strict matching of the SLA class. If no data plane tunnel is available that satisfies the SLA criteria, traffic is dropped. Note that for policy configured with this option, data traffic that matches the match conditions is dropped until the application-aware routing path is established.

<table>
<thead>
<tr>
<th>Command</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>action sla-class sla-class-name strict</code></td>
<td>SLA class name defined in policy sla-class command</td>
</tr>
<tr>
<td><code>action sla-class sla-class-name preferred-color color strict</code></td>
<td></td>
</tr>
<tr>
<td><code>action sla-class sla-class-name preferred-color colors strict</code></td>
<td></td>
</tr>
</tbody>
</table>

If more than one data plane tunnel satisfies an SLA class criteria, the Cisco device selects one of them by performing load-balancing across the equal paths.

### Default Action

A policy's default action defines how to handle packets that match none of the match conditions. For application-aware routing policy, if you do not configure a default action, all data packets are accepted and transmitted based on normal routing decisions, with no consideration of SLA.

To modify this behavior, include the `default-action sla-class sla-class-name` command in the policy, specifying the name of an SLA class you defined in the `policy sla-class` command.

When you apply an SLA class in a policy's default action, you cannot specify the `strict` option.

If no data plane tunnel satisfies the SLA class in the default action, the Cisco device selects one of the available tunnels by performing load-balancing across equal paths.

### Apply Application-Aware Routing Policy

For an application-aware route policy to take effect, you apply it to a list of sites in the overlay network:

```bash
vSmart(config)# apply-policy site-list list-name app-route-policy policy-name
```

When you apply the policy, you do not specify a direction (either inbound or outbound). Application-aware routing policy affects only the outbound traffic on the Cisco devices.

For all `app-route-policy` policies that you apply with `apply-policy` commands, the site IDs across all the site lists must be unique. That is, the site lists must not contain overlapping site IDs. An example of overlapping site IDs are those in the two site lists `site-list 1, site-id 1-100,` and `site-list 2 site-id 70-130`. Here, sites 70 through 100 are in both lists. If you were to apply these two site lists to two different `app-route-policy` policies, the attempt to commit the configuration on the Cisco vSmart Controller would fail.

The same type of restriction also applies to the following types of policies:

- Centralized control policy (`control-policy`)
- Centralized data policy (`data-policy`)
- Centralized data policy used for cflowd flow monitoring (`data-policy` hat includes a `cflowd` action and `apply-policy` that includes a `cflowd-template` command)
You can, however, have overlapping site IDs for site lists that you apply for different types of policy. For example, the sites lists for `app-route-policy` and `data-policy` policies can have overlapping site IDs. So for the two example site lists above, `site-list 1, site-id 1-100`, and `site-list 2 site-id 70-130`, you could apply one to a control policy and the other to a data policy.

As soon as you successfully activate the configuration on the Cisco vSmart Controller by issuing a `commit` command, the controller pushes the application-aware routing policy to the Cisco devices at the specified sites.

To view the policy configured on the Cisco vSmart Controller, use the `show running-config` command on the controller.

To view the policy that the Cisco vSmart Controller has pushed to the Cisco device, issue the `show policy from-vsmart` command on the router.

To display flow information for the application-aware applications running on the Cisco device, issue the `show app dpi flows` command on the router.

**How Application-Aware Routing Policy Is Applied in Combination with Other Data Policies**

If you configure a Cisco device with application-aware routing policy and with other policies, the policies are applied to data traffic sequentially.

On a Cisco device, you can configure the following types of data policy:

- **Centralized data policy.** You configure this policy on the Cisco vSmart Controller, and the policy is passed to the Cisco device. You define the configuration with the `policy data-policy configuration` command, and you apply it with the `apply-policy site-list data-policy`, or `apply-policy site-list vpn-membership` command.

- **Localized data policy, which is commonly called access lists.** You configure access lists on the Cisco device with the `policy access-list` configuration command. You apply them, within a VPN, to an incoming interface with the `vpn interface access-list in` configuration command or to an outgoing interface with the `vpn interface access-list out` command.

- **Application-aware routing policy.** Application-aware routing policy affects only traffic that is flowing from the service side (the local/LAN side) to the tunnel (WAN side) of the Cisco device. You configure application-aware routing policy on the Cisco vSmart Controller with the `policy app-route-policy` configuration command, and you apply it with the `apply-policy site-list app-route-policy` command. When you commit the configuration, the policy is passed to the appropriate Cisco devices. Then, matching data traffic on the Cisco device is processed in accordance with the configured SLA conditions. Any data traffic that is not dropped as a result of this policy is passed to the data policy for evaluation. If the data traffic does not match and if no default action is configured, transmit it without SLA consideration.

You can apply only one data policy and one application-aware routing policy to a single site in the overlay network. When you define and apply multiple site lists in a configuration, you must ensure that a single data policy or a single application-aware routing policy is not applied to more than one site. The CLI does not check for this circumstance, and the `validate` configuration command does not detect whether multiple policies of the same type are applied to a single site.

For data traffic flowing from the service side of the router to the WAN side of the router, policy evaluation of the traffic evaluation occurs in the following order:

1. Apply the input access list on the LAN interface. Any data traffic that is not dropped as a result of this access list is passed to the application-aware routing policy for evaluation.
2. Apply the application-aware routing policy. Any data traffic that is not dropped as a result of this policy is passed to the data policy for evaluation. If the data traffic does not match and if no default action is configured, transmit it without SLA consideration.

3. Apply the centralized data policy. Any data traffic that is not dropped as a result of the input access list is passed to the output access list for evaluation.

4. Apply the output access list on the WAN interface. Any data traffic that is not dropped as a result of the output access list is transmitted out the WAN interface.

For data traffic coming from the WAN through the router and into the service-side LAN, the policy evaluation of the traffic occurs in the following order:

1. Apply the input access list on the WAN interface. Any data traffic that is not dropped as a result of the input access list is passed to the data policy for evaluation.

2. Apply the data policy. Any data traffic that is not dropped as a result of the input access list is passed to the output access list for evaluation.

3. Apply the output access list on the LAN interface. Any data traffic that is not dropped as a result of the output access list is transmitted out the LAN interface, towards its destination at the local site.

As mentioned above, application-aware routing policy affects only traffic that is flowing from the service side (the local/LAN side) to the tunnel (WAN) side of the Cisco device, so data traffic inbound from the WAN is processed only by access lists and data policy.

## Configure the Monitoring of Data Plane Tunnel Performance

The Bidirectional Forwarding Detection (BFD) protocol runs over all data plane tunnels between Cisco devices, monitoring the liveness, and network and path characteristics of the tunnels. Application-aware routing uses the information gathered by BFD to determine the transmission performance of the tunnels. Performance is reported in terms of packet latency and packet loss on the tunnel.

BFD sends Hello packets periodically to test the liveness of a data plane tunnel and to check for faults on the tunnel. These Hello packets provide a measurement of packet loss and packet latency on the tunnel. The Cisco device records the packet loss and latency statistics over a sliding window of time. BFD keeps track of the six most recent sliding windows of statistics, placing each set of statistics in a separate bucket. If you configure an application-aware routing policy for the Cisco device, it is these statistics that the router uses to determine whether a data plane tunnel's performance matches the requirements of the policy's SLA.

The following parameters determine the size of the sliding window:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
<th>Configuration Command</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>BFD Hello packet interval</td>
<td>1 second</td>
<td><code>bfd color color hello-interval seconds</code></td>
<td>1 through 65535 seconds</td>
</tr>
<tr>
<td>Polling interval for application-aware routing</td>
<td>10 minutes</td>
<td><code>bfd app-route poll-interval milliseconds</code></td>
<td>1 through 4,294,967</td>
</tr>
<tr>
<td>Multiplier for application-aware routing</td>
<td>6</td>
<td><code>bfd app-route multiplier number</code></td>
<td>1 through 6</td>
</tr>
</tbody>
</table>
Let us use the default values for these parameters to explain how application-aware routing works:

- For each sliding window time period, application-aware routing sees 600 BFD Hello packets (BFD Hello interval x polling interval: 1 second x 600 seconds = 600 Hello packets). These packets provide measurements of packet loss and latency on the data plane tunnels.

- Application-aware routing retains the statistics for 1 hour (polling interval x multiplier: 10 minutes x 6 = 60 minutes).

- The statistics are placed in six separate buckets, indexed with the numbers 0 through 5. Bucket 0 contains the latest statistics, and bucket 5 the oldest. Every 10 minutes, the newest statistics are placed in bucket 0, the statistics in bucket 5 are discarded, and the remaining statistics move into the next bucket.

- Every 60 minutes (every hour), application-aware routing acts on the loss and latency statistics. It calculates the mean of the loss and latency of all the buckets in all the sliding windows and compares this value to the specified SLAs for the tunnel. If the calculated value satisfies the SLA, application-aware routing does nothing. If the value does not satisfy the SLA, application-aware routing calculates a new tunnel.

- Application-aware routing uses the values in all six buckets to calculate the mean loss and latency for a data tunnel. This is because the multiplier is 6. While application-aware always retains six buckets of data, the multiplier determines how many it actually uses to calculate the loss and latency. For example, if the multiplier is 3, buckets 0, 1, and 2 are used.

Because these default values take action only every hour, they work well for a stable network. To capture network failures more quickly so that application-aware routing can calculate new tunnels more often, adjust the values of these three parameters. For example, if you change just the polling interval to 1 minute (60,000 milliseconds), application-aware routing reviews the tunnel performance characteristics every minute, but it performs its loss and latency calculations based on only 60 Hello packets. It may take more than 1 minute for application-aware routing to reset the tunnel if it calculates that a new tunnel is needed.

To display the next-hop information for an IP packet that a Cisco device sends out a service side interface, use the `show policy service-path` command. To view the similar information for packets that the router sends out a WAN transport tunnel interface, use the `show policy tunnel-path` command.

### Enable Application Visibility on Cisco Devices

You can enable application visibility directly on Cisco devices, without configuring application-aware routing policy so that you can monitor all the applications running in all VPNs in the LAN. To do this, configure application visibility on the router:

```vEdge(config)# policy app-visibility```

To monitor the applications, use the `show app dpi applications` and `show app dpi supported-applications` commands on the Cisco device.

### Application-Aware Routing Policy Configuration Example

This topic shows a straightforward example of configuring application-aware routing policy. This example defines a policy that applies to ICMP traffic, directing it to links with latency of 50 milliseconds or less when such links are available.
Configuration Steps

You configure application-aware routing policy on a Cisco vSmart Controller. The configuration consists of the following high-level components:

- Definition of the application (or applications)
- Definition of SLA parameters
- Definition of sites, prefixes, and VPNs
- Application-aware routing policy itself
- Specification of overlay network sites to which the policy is applied

The order in which you configure these components is immaterial from the point of view of the CLI. However, from an architectural design point of view, a logical order is to first define all the parameters that are invoked in the application-aware routing policy itself or that are used to apply the policy to various sites in the overlay network. Then, you specify the application-aware routing policy itself and the network sites to which you want to apply the policy.

Here is the procedure for configuring this application-aware routing policy on a Cisco vSmart Controller:

1. Define the SLA parameters to apply to matching ICMP traffic. In our example, we want to direct ICMP traffic to links that have a latency of 50 milliseconds or less:

   ```
   vSmart# config
   vSmart(config)# policy sla-class test_sla_class latency 50
   vSmart(config-sla-class-test_sla_class)#
   ```

2. Define the site and VPN lists to which we want to apply the application-aware routing policy:

   ```
   vSmart(config-sla-class-test_sla_class)# exit
   vSmart(config-sla-class-test_sla_class)# lists vpn-list vpn_1_list vpn 1
   vSmart(config-vpn-list-vpn_1_list)# exit
   vSmart(config-lists)# site-list site_500 site-id 500
   ```

3. Configure the application-aware routing policy. Note that in this example, we apply the policy to the application in two different ways: In sequences 1, 2, and 3, we specify the protocol number (protocol 1 is ICMP, protocol 6 is TCP, and protocol 17 is UDP).

   ```
   vSmart(config-site-list-site_500)# exit
   vSmart(config-lists)# exit
   vSmart(config-policy)# app-route-policy test_app_route_policy
   vSmart(config-app-route-policy-test_app_route_policy)# vpn-list vpn_1_list
   vSmart(config-vpn-list-vpn_1_list)# sequence 1 match protocol 6
   vSmart(config-match)# exit
   vSmart(config-sequence-1)# action sla-class test_sla_class strict
   vSmart(config-match)# exit
   vSmart(config-vpn-list-vpn_1_list)# sequence 2 match protocol 17
   vSmart(config-match)# exit
   vSmart(config-sequence-2)# action sla-class test_sla_class
   vSmart(config-sequence-2)# exit
   vSmart(config-vpn-list-vpn_1_list)# sequence 3 match protocol 1
   vSmart(config-match)# exit
   vSmart(config-sequence-3)# action sla-class test_sla_class strict
   vSmart(config-sequence-3)# exit
   vSmart(config-sequence-4)#
   ```

4. Apply the policy to the desired sites in the Cisco SD-WAN overlay network:
vSmart(config-sequence-4)# top
vSmart(config)# apply-policy site-list site_500 app-route-policy test_app_route_policy

5. Display the configuration changes:
   vSmart(config-site-list-site_500)# top
   vSmart(config)# show config

6. Validate that the configuration contains no errors:
   vSmart(config)# validate
   Validation complete

7. Activate the configuration:
   vSmart(config)# commit
   Commit complete.

8. Exit from configuration mode:
   vSmart(config)# exit
   vSmart#

**Full Example Configuration**

Putting all the pieces of the configuration together gives this configuration:

vSmart# show running-config policy
policy
  sla-class test_sla_class
    latency 50
  !
  app-route-policy test_app_route_policy
  vpn-list vpn_1_list
    sequence 1
      match
        protocol 6
        !
      action sla-class test_sla_class strict
        !
    sequence 2
      match
        protocol 17
        !
      action sla-class test_sla_class
        !
    sequence 3
      match
        protocol 1
        !
      action sla-class test_sla_class strict
        !
    !
  lists
  vpn-list vpn_1_list
    vpn 1
    !
  site-list site_500
    site-id 500
    !
  site-list site_600
    site-id 600
    !
Application-Aware Routing Policy Configuration Example

!  
! apply-policy
  site-list site_500
  app-route-policy test_app_route_policy
!  
!
Service Chaining

Service chaining allows data traffic to be rerouted through one or more services, such as firewall, load balancer, and intrusion detection and prevention (IDP) devices.

Services in the Network

Services such as firewall, load balancer, and intrusion detection and prevention (IDP) are often run within a virtualized environment, and they may physically be centralized in one location or in several locations for redundancy. Services may be internal, cloud based, or external subscriptions. Networks must be able to reroute traffic from any location in the network through such services.

Customers want the ability to internally spawn or externally subscribe to new services on demand—for capacity, redundancy, or simply to select best-of-breed technologies. For example, if a firewall site exceeds its capacity, a customer can spawn new firewall service at a new location. Supporting this new firewall would require the configuration of policy-based, weighted load distribution to multiple firewalls.

Following are some of the reasons to reroute a traffic flow through a service or chain of services:

- Traffic flow from a less secure region of a network must pass through a service, such as a firewall, or through a chain of services to ensure that it has not been tampered with.
- For a network that consists of multiple VPNs, each representing a function or an organization, traffic between VPNs must traverse through a service, such as a firewall, or through a chain of services. For example, in a campus, interdepartmental traffic might go through a firewall, while intradepartmental traffic might be routed directly.
- Certain traffic flows must traverse a service, such as a load balancer.

Today, the only way to reroute traffic flow is by provisioning every routing node—from the source to the service node to the systems beyond the service node—with a policy route. This is done either by having an operator manually configure each node or by using a provisioning tool that performs the configuration for each node on behalf of the operator. Either way, the process is operationally complex to provision, maintain, and troubleshoot.

Provisioning Services in the Cisco SD-WAN Overlay Network

In the Cisco SD-WAN solution, the network operator can enable and orchestrate all service chaining from a central controller, that is, from the Cisco vSmart controller. No configuration or provisioning is required at any of the Cisco vEdge devices.

The general flow of service chaining in a Cisco SD-WAN network is as follows:
- vEdge routers advertise the services available in their branch or campus—such as firewall, IDS, and IDP—to the Cisco vSmart controllers in their domain. Multiple Cisco vEdge devices can advertise the same services.

- Cisco vEdge devices also advertise their OMP routes and TLOCs to the Cisco vSmart controllers.

- For traffic that require services, policy on the Cisco vSmart controller changes the next hop for the OMP routes to the service landing point. In this way, the traffic is first processed by the service before being routed to its final destination.

The following figure illustrates how service chaining works in the Cisco SD-WAN solution. The network shown has a centralized vEdge hub router that is connected to two branches, each with a Cisco vEdge device. The standard network design implements a control policy such that all traffic from branch site 1 to branch site 2 travels through the vEdge hub router. Sitting behind the hub router is a firewall device. So now, assume we want all traffic from site 1 to site 2 to first be processed by the firewall. Traffic from the Cisco vEdge device at site 1 still flows to the vEdge hub router, but instead of sending it directly to site 2, the hub router redirects the traffic to the firewall device. When the firewall completes its processing, it returns all cleared traffic to the hub, which then passes it along to the Cisco vEdge device at site 2.

**Service Route SAFI**

The hub and local branch Cisco vEdge devices advertise the services available in their networks to the Cisco vSmart controllers in its domain using service routes, which are sent via OMP using the service route Subsequent Address Family Identifier (SAFI) bits of the OMP NLRI. The Cisco vSmart controllers maintain the service routes in their RIB, and they do not propagate these routes to the vEdges.

Each service route SAFI has the following attributes:

- VPN ID (vpn-id)—Identifies the VPN that the service belongs to.

- Service ID (svc-id)—Identifies the service being advertised by the service node. The Cisco SD-WAN software has the following predefined services:
• FW, for firewall (maps to svc-id 1)
• IDS, for Intrusion Detection Systems (maps to svc-id 2)
• IDP, for Identity Providers (maps to svc-id 3)
• netsvc1, netsvc2, netsvc3, and netsvc4, which are reserved for custom services (they map to svc-id 4, 5, 6, and 7, respectively)

• Label—For traffic that must traverse a service, the Cisco vSmart replaces the label in the OMP route with the service label in order to direct the traffic to that service.
• Originator ID (originator-id)—The IP address of the service node that is advertising the service.
• TLOC—The transport location address of the vEdge that is “hosting” the service.
• Path ID (path-id)—An identifier of the OMP path.

Service Chaining Policy

To route traffic through a service, you provision either a control policy or a data policy on the Cisco vSmart controller. You use a control policy if the match criteria are based on a destination prefix or any of its attributes. You use a data policy if the match criteria include the source address, source port, DSCP value, or destination port of the packet or traffic flow. You can provision the policy directly via CLI, or it can be pushed from the vManage management system.

The Cisco vSmart controller maintains OMP routes, TLOC routes, and service routes in its route table. A given OMP route carries a TLOC and the label associated with it. On a Cisco vSmart controller, a policy can be applied that changes the TLOC and its associated label to be that of a service.

Service Chaining Configuration Examples

Service chaining control policies direct data traffic to service devices that can be located in various places in the network before the traffic is delivered to its destination. For service chaining to work, you configure a centralized control policy on the Cisco vSmart Controller, and you configure the service devices themselves on the Cisco vEdge device collocated in the same site as the device. To ensure that the services are advertised to the Cisco vSmart Controller, the IP address of the service device must resolve locally.

This topic provides examples of configuring service chaining.
Route Intersite Traffic through a Service

A simple example is to route data traffic traveling from one site to another through a service. In this example, we route all traffic traveling from the Cisco vEdge device at Site 1 to the Cisco vEdge device at Site 2 through a firewall service that sits behind a vEdge hub (whose system IP address is 100.1.1.1). To keep things simple, all devices are in the same VPN.

For this scenario, you configure the following:

- On the vEdge hub router, you configure the IP address of the firewall device.
- On the Cisco vSmart Controller, you configure a control policy that redirects traffic destined from Site 1 to Site 2 through the firewall service.
- On the Cisco vSmart Controller, you apply the control policy to Site 1.

Here is the configuration procedure:

1. On the vEdge hub router, provision the firewall service, specifying the IP address of the firewall device. With this configuration, OMP on the vEdge hub router advertises one service route to the Cisco vSmart Controller. The service route contains a number of properties that identify the location of the firewall, including the TLOC of the vEdge hub router and a service label of svc-id-1, which identifies the service type as a firewall. (As mentioned above, before advertising the route, the Cisco vEdge device ensures that the firewall's IP address can be resolved locally.)

   ```
   vpn 10
   service FW address 1.1.1.1
   ```

2. On the Cisco vSmart Controller, configure a control policy that redirects data traffic traveling from Site 1 to Site 2 through the firewall. Then, also on the Cisco vSmart Controller, apply this policy to Site 1.

   ```
   policy
   lists
   site-list firewall-sites
   ```
This policy configuration does the following:

- Create a site list called `firewall-sites` that is referenced in the `apply-policy` command and that enumerates all the sites that this policy applies to. If you later want to scale this policy so that all traffic destined to Site 2 from other sites should also first pass through the firewall, all you need to do is add the additional site IDs to the `firewall-sites` site list. You do not need to change anything in the `control-policy firewall-service` portion of the configuration.

- Define a control policy named `firewall-service`. This policy has one sequence element and the following conditions:

  - Match routes destined for Site 2.
  - If a match occurs, accept the route and redirect it to the firewall service provided by the vEdge Hub router, which is located in VPN 10.
  - Accept all nonmatching traffic. That is, accept all traffic not destined for Site 2.

- Apply the policy to the sites listed in `firewall-list`, that is, to Site 1. The Cisco vSmart controller applies the policy in the outbound direction, that is, on routes that it redistributes to Site 1. In these routes:

  - The TLOC is changed from Site 2’s TLOC to the vEdge hub router’s TLOC. This is the TLOC that the Cisco vSmart Controller learned from the service route received from the vEdge hub router. It is because of the change of TLOC that traffic destined for Site 2 is directed to the vEdge hub router.
  - The label is changed to svc-id-1, which identifies the firewall service. This label causes the vEdge hub router to direct the traffic to the firewall device.

When the vEdge hub router receives the traffic, it forwards it to the address 1.1.1.1, which is the system IP address of the firewall. After the firewall has finished processing the traffic, the firewall returns the traffic to the vEdge hub router, and this router then forwards it to its final destination, which is Site 2.
Route Inter-VPN Traffic through a Service Chain with One Service per Node

A service chain allows traffic to pass through two or more services before reaching its destination. The example here routes traffic from one VPN to another through services located in a third VPN. The services are located behind different vEdge hub routers. Specifically, we want all traffic from vEdge-1 in VPN 20 and that is destined for prefix x.x.0.0/16 in VPN 30 on vEdge-2 to go first through the firewall behind vEdge Hub-1 and then through the custom service netsvc1 behind vEdge Hub-2 before being sent to its final destination.

For this policy to work:

- VPN 10, VPN 20, and VPN 30 must be connected by an extranet, such as the Internet
- VPN 10 must import routes from VPN 20 and VPN 30. Routes can be selectively imported if necessary.
- VPN 20 must import routes from VPN 30. Routes can be selectively imported if necessary.
- VPN 30 must import routes from VPN 20. Routes can be selectively imported if necessary.

For this scenario, you configure four things:

- You configure the IP address of the firewall device on the vEdge Hub-1 router.
- You configure the IP address of the custom service device on the vEdge Hub-2 router.
- On the Cisco vSmart Controller, you configure a control policy that redirects traffic destined from Site 1 to Site 2 through the firewall device.
- On the Cisco vSmart Controller, you configure a second control policy that redirects traffic to the custom service device.

Here is the configuration procedure:

1. Configure the firewall service on vEdge Hub-1. With this configuration, OMP on the vEdge Hub-1 router advertises a service route to the Cisco vSmart Controller. The service route contains a number of properties
that identify the location of the firewall, including the TLOC of the vEdge hub router and a service label of svc-id-1, which identifies the service type as a firewall.

```
vpn 10
  service fw address 1.1.1.1
```

2. Configure the custom service netsvc1 on vEdge Hub-2. With this configuration, OMP on the vEdge Hub-2 router advertises a service route to the vSmart controller. The service route contains the TLOC of the vEdge Hub-2 and a service label of svc-id-4, which identifies the custom service.

```
vpn 10
  service netsvc1 address 2.2.2.2
```

3. Create a control policy on the Cisco vSmart Controller for first service in the chain—the firewall—and apply it to Site 1, which is the location of the vEdge-1 router:

```
policy
  lists
    site-list firewall-custom-service-sites
      site-id 1
  control-policy firewall-service
    sequence 10
    match route
      vpn 30
      site-id 2
    action accept
      set service FW
    default-action accept
  apply-policy
    site-list firewall-custom-service-sites control-policy firewall-service out
```

This policy configuration does the following:

- Create a site list called `firewall-custom-service-sites` that is referenced in the `apply-policy` command and that enumerates all the sites that this policy applies to.

- Define a control policy named `firewall-service` that has one sequence element and the following conditions:
  - Match routes destined for both VPN 30 and Site 2.
  - If a match occurs, accept the route and redirect it to a firewall service.
  - If a match does not occur, accept the traffic.

- Apply the policy to the sites in the `firewall-custom-service-sites` site list, that is, to Site 1. The Cisco vSmart controller applies this policy in the outbound direction, that is, on routes that it redistributes to Site 1. In these routes:
  - The TLOC is changed from Site 2’s TLOC to the vEdge Hub-1 router’s TLOC. This is the TLOC that the Cisco vSmart Controller learned from the service route received from the vEdge hub. It is because of the change of TLOC that traffic destined for Site 2 is directed to the vEdge Hub-1 router.
  - The label is changed to svc-id-1, which identifies the firewall service. This label causes the vEdge Hub-1 router to direct the traffic to the firewall device.

When the vEdge Hub-1 router receives the traffic, it forwards it to the address 1.1.1.1, which is the system IP address of the firewall. After the firewall completes processing the traffic, it returns the traffic to the
vEdge Hub-1 router, which, because of the policy defined in the next step, forwards it to the vEdge Hub-2 router.

4. Create a control policy on the Cisco vSmart Controller for the second service in the chain, which is the custom service, and apply it to Site 3, which is the location of the vEdge Hub-2 router:

```bash
policy
  site-list custom-service
  site-id 3
control-policy netsvc1-service
  sequence 10
  match route
    vpn 30
    site-id 2
  action accept
    set service netsvc1
default-action accept
apply-policy
  site-list custom-service control-policy netsvc1-service out
```

This policy configuration does the following:

- Create a site list called `custom-service` that is referenced in the `apply-policy` command and that enumerates all the sites that this policy applies to.

- Define a control policy named `netsvc1-service` that has one sequence element and the following conditions:
  - Match routes destined for both VPN 30 and Site 2.
  - If a match occurs, accept the route and redirect it to the custom service.
  - If a match does not occur, accept the traffic.

- Apply the policy to the sites in the `custom-service` list, that is, to Site 3. The Cisco vSmart controller applies this policy in the outbound direction, that is, on routes that it redistributes to Site 3. In these routes:
  - The TLOC is changed from Site 2’s TLOC to the vEdge Hub-2 router’s TLOC. This is the TLOC that the Cisco vSmart Controller learned from the service route received from the vEdge Hub-2 router. It is because of the change of TLOC that traffic destined for Site 2 is directed to the vEdge Hub-2 router.
  - The label is changed to svc-id-4, which identifies the custom service. This label causes the vEdge Hub-2 to direct the traffic to the device that is hosting the custom service.

When the vEdge Hub-2 routers receives the traffic, it forwards it to the address 2.2.2.2, which is the system IP address of the device hosting the custom service. After the traffic has been processed, it is returned to the vEdge Hub-2 router, which then forwards it to its final destination, Site 2.
If a service chain has more than one service that is connected to the same node, that is, both services are behind the same Cisco vEdge device, you use a combination of control policy and data policy to create the desired service chain. The example here is similar to the one in the previous section, but instead has a firewall and a custom service (netsvc-1) behind a single vEdge hub router. Here, we want all data traffic from vEdge-1 in VPN 20 destined for prefix x.x.0.0/16 on vEdge-2 in VPN 30 to first go through the firewall at vEdge Hub-1, then through the custom service netsvc1, also at vEdge Hub-1, and then to its final destination.

For this policy to work:

- VPN 10, VPN 20, and VPN 30 must be connected by an extranet, such as the Internet.
- VPN 10 must import routes from VPN 20 and VPN 30. Routes can be selectively imported if necessary.
- VPN 20 must import routes from VPN 30. Routes can be selectively imported if necessary.
- VPN 30 must import routes from VPN 20. Routes can be selectively imported if necessary.

For this scenario, you configure the following:

- On the vEdge hub router, you configure the firewall and custom services.
- On the Cisco vSmart Controller, you configure a control policy that redirects data traffic from Site 1 that is destined to Site 2 through the firewall.
- On the Cisco vSmart Controller, you configure a data policy that redirects data traffic to the custom service.

Here is the configuration procedure:

1. On the vEdge hub router, configure the firewall and custom services:
VPN 10
service FW address 1.1.1.1
service netsvc1 address 2.2.2.2

With this configuration, OMP on the vEdge hub router advertises two service routes to the Cisco vSmart Controller, one for the firewall and the second for the custom service netsvc1. Both service routes contain the TLOC of the vEdge Hub-1 router and a service label that identifies the type of service. For the firewall service, the label is svc-id-1, and for the custom service, the label is svc-id-4.

2. On the Cisco vSmart Controller, configure a control policy controller to reroute traffic destined for VPN 30 (at Site 2) to firewall service that is connected to vEdge Hub-1 (at Site 3), and apply this policy to Site 1:

   ```
   policy
   lists
   site-list vEdge-1
   site-id 1
   control-policy firewall-service
   sequence 10
   match route
   vpn 30
   action accept
   set service FW
   apply-policy
   site-list vEdge-1 control-policy firewall-service out
   ```

3. On the Cisco vSmart Controller, configure a data policy that redirects, or chains, the data traffic received from the firewall device to the custom service netsvc1. Then apply this policy to vEdge Hub-1. This data policy routes packets headed for destinations in the network x.x.0.0/16 to the IP address 2.2.2.2, which is the system IP address of the device hosting the custom service.

   ```
   policy
   lists
   site-list vEdge-2
   site-id 2
   site-list vEdge-Hub-1
   site-id 3
   prefix-list svc-chain
   ip-prefix x.x.0.0/16
   vpn-list vpn-10
   vpn 10
   data-policy netsvc1-policy
   vpn-list vpn-10
   sequence 1
   match
   ip-destination x.x.0.0/16
   action accept
   set next-hop 2.2.2.2
   apply-policy
   site-list vEdge-Hub-1 data-policy netsvc1-policy from-service
Traffic Flow Monitoring with Cflowd

Cflowd monitors traffic flowing through Cisco vEdge devices and Cisco XE SD-WAN devices in the overlay network and exports flow information to a collector, where it can be processed by an IPFIX analyzer. For a traffic flow, cflowd periodically sends template reports to the flow collector. These reports contain information about the flows and the data is extracted from the payload of these reports.

You can create a cflowd-template that defines the location of cflowd collectors, how often sets of sampled flows are sent to the collectors, and how often the template is sent to the collectors (on Cisco vSmart Controllers only). You can configure a maximum of four cflowd collectors per Cisco device. To have a cflowd-template take effect, apply it with the appropriate data policy.

You must configure at least one cflowd-template, but it need not contain any parameters. With no parameters, the data flow cache on the nodes is managed using default settings, and no flow export occurs.

Cflowd traffic flow monitoring is equivalent to Flexible Netflow (FNF).

The cflowd software implements cflowd version 10, as specified in RFC 7011 and RFC 7012. Cflowd version 10 is also called the IP Flow Information Export (IPFIX) protocol.

Cflowd performs 1:1 sampling. Information about all flows is aggregated in the cflowd records; flows are not sampled. Cisco devices do not cache any of the records that are exported to a collector.

Components of Cflowd

In the overlay network, you configure cflowd using a centralized data policy. As part of the policy, you specify the location of the collector.

By default, flow information is sent to the collector every 60 seconds. You can modify this and other timers related to how often cflowd templates are refreshed and how often a traffic flow times out.
You can configure many cflowd policies, but in one single cflowd policy, you can configure at most four external collectors. When you configure a new data policy that changes which flows are sampled, the software allows the old flows to expire gracefully rather than deleting them all at once.

The Cisco device exports template records and data records to a collector. The template record is used by the collector to parse the data record information that is exported to it.

---

**Note**

Option templates are not supported on Cisco vEdge devices.

---

The source IP address for the packet containing the IPFIX records is selected from the collector that is closer to the interfaces in the VPN. The flow records are exported through TCP or UDP connections for Cisco devices. Anonymization of records and TLS encryption are not performed, because it is assumed that the collector and the IPFIX analyzer are both located within the data center, traffic traveling within the data center is assumed to be safe.

Cflowd can track GRE, ICMP, IPsec, SCTP, TCP, and UDP flows.

**IPFIX Information Elements Exported to the Collector**

The Cisco SD-WAN cflowd software exports the following 22 IPFIX information elements to the cflowd collector. These information elements are a subset of those defined in *RFC 7012* and maintained by IANA. The elements are exported in the order listed. You cannot modify the information elements that are exported, nor can you change the order in which they appear.

### Table 31:

<table>
<thead>
<tr>
<th>Information Element</th>
<th>Element ID</th>
<th>Description</th>
<th>Data Type</th>
<th>Data Type Semantics</th>
<th>Units or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN Identifier</td>
<td>Enterprise specific</td>
<td>Cisco SD-WAN VPN identifier. Cisco SD-WAN uses the enterprise ID for VIP_IANA_ENUM or 41916, and the VPN element ID is 4321.</td>
<td>unsigned32 (4 bytes)</td>
<td>identifier</td>
<td>0 through 65535</td>
</tr>
<tr>
<td>sourceIPv4Address</td>
<td>8</td>
<td>IPv4 source address in the IP packet header.</td>
<td>ipv4Address (4 bytes)</td>
<td>default</td>
<td>—</td>
</tr>
<tr>
<td>destinationIPv4Address</td>
<td>12</td>
<td>IPv4 destination address in the IP packet header.</td>
<td>IPv4Address (4 bytes)</td>
<td>default</td>
<td>—</td>
</tr>
<tr>
<td>ipDiffServCodePoint</td>
<td>195</td>
<td>Value of a Differentiated Services Code Point (DSCP) encoded in the Differentiated Services field. This field spans the most significant 6 bits of the IPv4 TOS field.</td>
<td>unsigned8 (1 byte)</td>
<td>identifier</td>
<td>0 through 63</td>
</tr>
<tr>
<td>destinationTransportPort</td>
<td>11</td>
<td>Destination port identifier in the transport header. For the transport protocols UDP, TCP, and SCTP, this is the destination port number given in the respective header.</td>
<td>unsigned16 (2 bytes)</td>
<td>identifier</td>
<td>—</td>
</tr>
<tr>
<td>Information Element</td>
<td>Element ID</td>
<td>Description</td>
<td>Data Type</td>
<td>Data Type Semantics</td>
<td>Units or Range</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------------------</td>
<td>---------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>sourceTransportPort</td>
<td>7</td>
<td>Source port identifier in the transport header. For the transport protocols UDP, TCP, and SCTP, this is the destination port number given in the respective header. For GRE and IPsec flows, the value of this field is 0.</td>
<td>unsigned16 (2 bytes)</td>
<td>identifier</td>
<td>—</td>
</tr>
<tr>
<td>protocolIdentifier</td>
<td>4</td>
<td>Value of the protocol number in the Protocol field of the IP packet header. The protocol number identifies the IP packet payload type. Protocol numbers are defined in the IANA Protocol Numbers registry.</td>
<td>unsigned8 (1 byte)</td>
<td>identifier</td>
<td>—</td>
</tr>
<tr>
<td>flowStartSeconds</td>
<td>150</td>
<td>Absolute timestamp of the first packet of this flow.</td>
<td>dateTime-Seconds</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>flowEndSeconds</td>
<td>151</td>
<td>Absolute timestamp of the last packet of this flow.</td>
<td>dateTime-Seconds</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>octetTotalCount</td>
<td>85</td>
<td>Total number of octets in incoming packets for this flow at the observation point since initialization or re-initialization of the metering process for the observation point. The count includes the IP headers and the IP payload.</td>
<td>unsigned64 (8 bytes)</td>
<td>totalCounter</td>
<td>Octets</td>
</tr>
<tr>
<td>octetDeltaCount</td>
<td>1</td>
<td>Number of octets since the previous report in incoming packets for this flow at the observation point. This number includes IP headers and IP payload.</td>
<td>unsigned64 (8 bytes)</td>
<td>deltaCounter</td>
<td>Octets</td>
</tr>
<tr>
<td>packetTotalCount</td>
<td>86</td>
<td>Total number of incoming packets for this flow at the observation point since initialization or re-initialization of the metering process for the observation point.</td>
<td>unsigned64 (8 bytes)</td>
<td>totalCounter</td>
<td>Packets</td>
</tr>
<tr>
<td>packetDeltaCount</td>
<td>2</td>
<td>Number of incoming packets since the previous report for this flow at this observation point.</td>
<td>unsigned64 (8 bytes)</td>
<td>deltaCounter</td>
<td>Packets</td>
</tr>
<tr>
<td>tcpControlBits</td>
<td>6</td>
<td>TCP control bits observed for the packets of this flow. This information is encoded as a bit field; each TCP control bit has a bit in this set. The bit is set to 1 if any observed packet of this flow has the corresponding TCP control bit set to 1. Otherwise, the bit is set to 0. For values of this field, see the IANA IPFIX web page.</td>
<td>unsigned16 (2 bytes)</td>
<td>flags</td>
<td>—</td>
</tr>
<tr>
<td>maximumIpTotalLength</td>
<td>26</td>
<td>Length of the largest packet observed for this flow. The packet length includes the IP headers and the IP payload.</td>
<td>unsigned64 (8 bytes)</td>
<td>—</td>
<td>Octets</td>
</tr>
</tbody>
</table>
Configure Cflowd Traffic Flow Monitoring

This topic provides general procedures for configuring cflowd traffic flow monitoring. You configure cflowd traffic flow monitoring using the basic components of centralized data policy. You configure cflowd template options, including the location of the cflowd collector (if you are sending the flow to a collector), and you must configure cflowd as an action in the data policy.

To configure policy for cflowd traffic flow monitoring, use the Cisco vManage policy configuration wizard. The wizard consists of four sequential screens that guide you through the process of creating and editing policy components:

1. Create Applications or Groups of Interest—Create lists that group together related items and that you call in the match or action components of a policy.

<table>
<thead>
<tr>
<th>Information Element</th>
<th>Element ID</th>
<th>Description</th>
<th>Data Type</th>
<th>Data Type Semantics</th>
<th>Units or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>minimumIpTotalLength</td>
<td>25</td>
<td>Length of the smallest packet observed for this flow. The packet length includes the IP headers and the IP payload.</td>
<td>unsigned64 (8 bytes)</td>
<td>—</td>
<td>Octets</td>
</tr>
<tr>
<td>ipNextHopIPv4Address</td>
<td>15</td>
<td>IPv4 address of the next IPv4 hop.</td>
<td>IPv4Address (4 bytes)</td>
<td>default</td>
<td>—</td>
</tr>
<tr>
<td>egressInterface</td>
<td>14</td>
<td>Index of the IP interface where packets of this flow are being sent.</td>
<td>unsigned32 (4 bytes)</td>
<td>default</td>
<td>—</td>
</tr>
<tr>
<td>ingressInterface</td>
<td>10</td>
<td>Index of the IP interface where packets of this flow are being received.</td>
<td>unsigned32 (4 bytes)</td>
<td>identifier</td>
<td>—</td>
</tr>
<tr>
<td>icmpTypeCodeIPv4</td>
<td>32</td>
<td>Type and Code of the IPv4 ICMP message. The combination of both values is reported as (ICMP type * 256) + ICMP code.</td>
<td>unsigned16 (2 bytes)</td>
<td>identifier</td>
<td>—</td>
</tr>
<tr>
<td>flowEndReason</td>
<td>136</td>
<td>Reason for the flow termination. For values of this field, see the IANA IPFIX web page.</td>
<td>unsigned8 (1 byte)</td>
<td>identifier</td>
<td>—</td>
</tr>
<tr>
<td>ipClassOfService</td>
<td>5</td>
<td>Value of type of service (TOS) field in the IPv4 packet header.</td>
<td>unsigned8 (1 byte)</td>
<td>identifier</td>
<td>—</td>
</tr>
<tr>
<td>ipPrecedence</td>
<td>196</td>
<td>Value of IP precedence. This value is encoded in the first 3 bits of the IPv4 TOS field.</td>
<td>unsigned8 (1 byte)</td>
<td>flags</td>
<td>0 through 7</td>
</tr>
<tr>
<td>paddingOctets</td>
<td>210</td>
<td>Value of this Information Element is always a sequence of 0x00 values.</td>
<td>octetArray</td>
<td>default</td>
<td>—</td>
</tr>
</tbody>
</table>

- Configure Cflowd Traffic Flow Monitoring, on page 204
- Configure Cflowd Traffic Flow Monitoring Using CLI, on page 210
- Structural Components of Policy Configuration for Cflowd, on page 212
- Apply and Enable Cflowd Policy, on page 215
- Cflowd Traffic Flow Monitoring Configuration Example, on page 216
2. Configure Topology—Create the network structure to which the policy applies.
3. Configure Traffic Rules—Create the match and action conditions of a policy.
4. Apply Policies to Sites and VPNS—Associate policy with sites and VPNs in the overlay network.

In the first three policy configuration wizard screens, you are creating policy components or blocks. In the last screen, you are applying policy blocks to sites and VPNs in the overlay network.

For the cflowd policy to take effect, you must activate the policy.

**Step 1: Start the Policy Configuration Wizard**

To start the policy configuration wizard:

1. In the Cisco vManage NMS, select the **Configure > Policies** screen. When you first open this screen, the Centralized Policy tab is selected by default.

2. Click **Add Policy**.

The policy configuration wizard opens, and the Create Applications or Groups of Interest screen is displayed.

**Step 2: Create Applications or Groups of Interest**

To create lists of applications or groups to use in cflowd policy:

1. Create new lists as described in the following table:

<table>
<thead>
<tr>
<th>List Type</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| Prefix    | a. In the left bar, click **Prefix**.  
|           | b. Click **New Prefix List**.  
|           | c. Enter a name for the list.  
|           | d. In the Add Prefix field, enter one or more data prefixes separated by commas.  
|           | e. Click **Add**. |

| Site      | a. In the left bar, click **Site**.  
|           | b. Click **New Site List**.  
|           | c. Enter a name for the list.  
|           | d. In the Add Site field, enter one or more site IDs separated by commas.  
<p>|           | e. Click <strong>Add</strong>. |</p>
<table>
<thead>
<tr>
<th>List Type</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| VPN       | a. In the left bar, click VPN.  
           | b. Click New VPN List.  
           | c. Enter a name for the list.  
           | d. In the Add VPN field, enter one or more VPN IDs separated by commas.  
           | e. Click Add. |

2. Click **Next** to Configure Topology in the wizard. When you first open this screen, the Topology tab is selected by default.

**Step 3: Configure the Network Topology**

To configure the network topology:

1. In the Topology tab, create a network topology as described in the following table:
### Policy Type

<table>
<thead>
<tr>
<th>Policy Type</th>
<th>Description</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| Hub and Spoke | Policy for a topology with one or more central hub sites and with spokes connected to a hub | a. In the Add Topology drop-down, select **Hub and Spoke**.  
b. Enter a name for the hub-and-spoke policy.  
c. Enter a description for the policy.  
d. In the VPN List field, select the VPN list for the policy.  
e. In the left pane, click **Add Hub and Spoke**. A hub-and-spoke policy component containing the text string My Hub-and-Spoke is added in the left pane.  
f. Double-click the **My Hub-and-Spoke** text string, and enter a name for the policy component.  
g. In the right pane, add hub sites to the network topology:  
   1. Click **Add Hub Sites**.  
   2. In the Site List Field, select a site list for the policy component.  
   3. Click **Add**.  
   4. Repeat Steps 7a, 7b, and 7c to add more hub sites to the policy component.  
h. In the right pane, add spoke sites to the network topology:  
   1. Click **Add Spoke Sites**.  
   2. In the Site List Field, select a site list for the policy component.  
   3. Click **Add**.  
   4. Repeat Steps 8a, 8b, and 8c to add more spoke sites to the policy component.  
i. Repeat Steps 5 through 8 to add more components to the hub-and-spoke policy.  
j. Click **Save Hub and Spoke Policy**.  

---

**Table 33:**
### Procedure Description Policy

<table>
<thead>
<tr>
<th><strong>Policy Type</strong></th>
<th><strong>Description</strong></th>
<th><strong>Procedure</strong></th>
</tr>
</thead>
</table>
| Mesh            | Partial-mesh or full-mesh region                      | **a.** In the Add Topology drop-down, select *Mesh.*  
**b.** Enter a name for the mesh region policy component.  
**c.** Enter a description for the mesh region policy component.  
**d.** In the VPN List field, select the VPN list for the policy.  
**e.** Click *New Mesh Region.*  
**f.** In the Mesh Region Name field, enter a name for the individual mesh region.  
**g.** In the Site List field, select one or more sites to include in the mesh region.  
**h.** Repeat Steps 5 through 7 to add more mesh regions to the policy.  
**i.** Click *Save Mesh Region.* |

2. To use an existing topology:  
   **a.** In the Add Topology drop-down, click *Import Existing Topology.* The Import Existing Topology popup displays.  
   **b.** Select the type of topology.  
   **c.** In the Policy drop-down, select the name of the topology.  
   **d.** Click *Import.*

3. Click *Next* to move to Configure Traffic Rules in the wizard. When you first open this screen, the Application-Aware Routing tab is selected by default.

### Step 4: Configure Traffic Rules

To configure traffic rules for cflowd policy:

1. In the Application-Aware Routing bar, select the *Cflowd* tab.

2. Click the *Add Policy* drop-down.


4. Configure timer parameters for the cflowd template:
   **a.** In the Active Flow Timeout field, specify how long to collect a set of flows on which traffic is actively flowing, a value from 30 through 3,600 seconds. The default is 600 seconds (10 minutes).
   **b.** In the Inactive Flow Timeout field, specify how long to wait to send a set of sampled flows to a collector for a flow on which no traffic is flowing, a value from 1 through 3,600 seconds. The default is 60 seconds (1 minute).
   **c.** In the Flow Refresh Interval field, specify how often to send the cflowd template record fields to the collector, a value from 60 through 86,400 seconds (1 minute through 1 day). The default is 90 seconds.
d. In the Sampling Interval field, specify how many packets to wait before creating a new flow, a value from 1 through 65,536 seconds. While you can configure any integer value, the software rounds the value down to the nearest power of 2.

5. Click Add New Collector, and configure the location of the cflowd collector. You can configure up to four collectors.
   a. In the VPN ID field, enter the number of the VPN in which the collector is located.
   b. In the IP Address field, enter the IP address of the collector.
   c. In the Port Number field, enter the collector port number. The default port is 4739.
   d. In the Transport Protocol drop-down, select the transport type to use to reach the collector, either TCP or UDP.
   e. In the Source Interface field, enter the name of the interface to use to send flows to the collector. It can be either a Gigabit Ethernet, a 10-Gigabit Ethernet interface (ge), or a loopback interface (loopback number).

6. Click Save Cflowd Policy.

7. Click Next to move to Apply Policies to Sites and VPNS in the wizard.

Step 5: Apply Policies to Sites and VPNs

To apply a policy block to sites and VPNS in the overlay network:

1. If you are already in the policy configuration wizard, skip to Step 6. Otherwise, in the Cisco vManage NMS, select the Configure > Policies screen. When you first open this screen, the Centralized Policy tab is selected by default.

2. Click Add Policy. The policy configuration wizard opens, and the Create Applications or Groups of Interest screen is displayed.

3. Click Next. The Network Topology screen opens, and in the Topology bar, the Topology tab is selected by default.

4. Click Next. The Configure Traffic Rules screen opens, and in the Application-Aware Routing bar, the Application-Aware Routing tab is selected by default.

5. Click Next. The Apply Policies to Sites and VPNS screen opens.

6. In the Policy Name field, enter a name for the policy. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (−), and underscores (_). It cannot contain spaces or any other characters.

7. In the Policy Description field, enter a description of the policy. It can contain up to 2048 characters. This field is mandatory, and it can contain any characters and spaces.

8. From the Topology bar, select the type of policy block. The table then lists policies that you have created for that type of policy block.

9. Click Add New Site List. Select one or more site lists, and click Add.

10. Click Preview to view the configured policy. The policy is displayed in CLI format.
11. Click Save Policy. The Configuration > Policies screen opens, and the policies table includes the newly created policy.

Step 6: Activate a Centralized Policy

Activating a cflowd policy sends that policy to all connected Cisco vSmart Controllers. To activate a cflowd policy:

1. In the Cisco vManage NMS, select the Configure > Policies screen. When you first open this screen, the Centralized Policy tab is selected by default.

2. Select a policy.

3. Click the More Actions icon to the right of the row, and click Activate. The Activate Policy popup opens. It lists the IP addresses of the reachable Cisco vSmart Controllers to which the policy is to be applied.

4. Click Activate.

Configure Cflowd Traffic Flow Monitoring Using CLI

Following are the high-level steps for configuring a cflowd centralized data policy to perform traffic monitoring and to export traffic flows to a collector:

1. Create a list of overlay network sites to which the cflowd centralized data policy is to be applied (in the apply-policy command):

```
vSmart(config)# policy
vSmart(config-policy)# lists site-list list-name
vSmart(config-lists-list-name)# site-id site-id
```

The list can contain as many site IDs as necessary. Include one site-id command for each site ID. For contiguous site IDs, you can specify a range of numbers separated with a dash (–). Create additional site lists, as needed.

2. Create a list of VPN for which the cflowd centralized data policy is to be configured (in the policy data-policy command):

```
vSmart(config)# policy lists
vSmart(config-lists)# vpn-list list-name
vSmart(config-lists-list-name)# vpn vpn-id
```

3. Create lists of IP prefixes, as needed:

```
vSmart(config)# policy lists
vSmart(config-lists)# prefix-list list-name
vSmart(config-lists-list-name)# ip-prefix prefix/length
```

4. Configure a cflowd template, and optionally, configure template parameters, including the location of the cflowd collector, the flow export timers, and the flow sampling interval:

```
vSmart(config)# policy cflowd-template template-name
vSmart(config-cflowd-template-template-name)# collector vpn vpn-id address ip-address
  port port-number transport-type (transport_tcp | transport_udp) source-interface interface-name
vSmart(config-cflowd-template-template-name)# flow-active-timeout seconds
vSmart(config-cflowd-template-template-name)# flow-inactive-timeout seconds
vSmart(config-cflowd-template-template-name)# template-refresh seconds
```
You must configure a cflowd template, but it need not contain any parameters. With no parameters, the data flow cache on router is managed using default settings, and no flow export occurs. You can configure one cflowd template per router, and it can export to a maximum of four collectors.

By default, an actively flowing data set is exported to the collector every 600 seconds (10 minutes), a data set for a flow on which no traffic is flowing is sent every 60 seconds (1 minute), and the cflowd template record fields (the three timer values) are sent to the collector every 90 seconds.

Also by default, a new flow is created immediately after an existing flow has ended. If you modify the configuration of the template record fields, the changes take effect only on flows that are created after the configuration change has been propagated to the router. Because an existing flow continues indefinitely, to have configuration changes take effect, clear the flow with the `clear app cflowd flows` command.

5. If you configure a logging action, configure how often to log packets to the syslog files:

   vEdge(config)# policy log-frequency number

6. Create a data policy instance and associate it with a list of VPNs:

   vSmart(config)# policy data-policy policy-name
   vSmart(config-data-policy-policy-name)# vpn-list list-name

7. Create a sequence to contain a single match–action pair:

   vSmart(config-vpn-list-list-name)# sequence number
   vSmart(config-sequence-number)#

   The match–action pairs are evaluated in order, by sequence number, starting with the lowest numbered pair and ending when the route matches the conditions in one of the pairs. If no match occurs, the default action is taken.

8. Define match parameters for the data packets:

   vSmart(config-sequence-number)# match parameters

9. In the action, enable cflowd:

   vSmart(config-sequence-number)# action cflowd

10. In the action, count or log data packets:

    vSmart(config-sequence-number)# action count counter-name
    vSmart(config-sequence-number)# action log

11. Create additional numbered sequences of match–action pairs within the data policy, as needed.

12. If a route does not match any of the conditions in one of the sequences, it is rejected by default. If you want nonmatching prefixes to be accepted, configure the default action for the policy:

    vSmart(config-policy-name)# default-action accept

13. Apply the policy and the cflowd template to one or more sites in the overlay network:

    vSmart(config)# apply-policy site-list list-name data-policy policy-name
    vSmart(config)# apply-policy site-list list-name cflowd-template template-name
Structural Components of Policy Configuration for Cflowd

Here are the structural components required to configure cflowd on a Cisco vSmart Controller. Each component is explained in more detail in the sections below.

```
policy
  lists
    prefix-list list-name
    ip-prefix prefix
    site-list list-name
    site-id site-id
    vpn-list list-name
    vpn vpn-id
  log-frequency number
  cflowd-template template-name
    collector vpn vpn-id address ip-address port port-number transport transport-type
    source-interface interface-name
    flow-active-timeout seconds
    flow-inactive-timeout seconds
    flow-sampling-interval number
    template-refresh seconds
  data-policy policy-name
    vpn-list list-name
    sequence number
    match
      match-parameters
    action
      cflowd
      count counter-name
      drop
      log
    default-action
      (accept | drop)
  apply-policy site-list list-name
  data-policy policy-name
  cflowd-template template-name
```

**Lists**

Centralized data policy uses the following types of lists to group related items. You configure lists under the `policy lists` command hierarchy on Cisco vSmart Controllers.

**Table 34:**

<table>
<thead>
<tr>
<th>List Type</th>
<th>Description</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data prefixes</td>
<td>List of one or more IP prefixes. To configure multiple prefixes in a single list, include multiple <code>ip-prefix</code> options, specifying one prefix in each option.</td>
<td><code>data-prefix-list</code> list-name &lt;br&gt;<code>ip-prefix</code> prefix/length</td>
</tr>
<tr>
<td>Sites</td>
<td>List of one or more site identifiers in the overlay network. To configure multiple sites in a single list, include multiple <code>site-id</code> options, specifying one site number in each option. You can specify a single site identifier (such as <code>site-id 1</code>) or a range of site identifiers (such as <code>site-id 1-10</code>).</td>
<td><code>site-list list-name</code> &lt;br&gt;<code>site-id site-id</code></td>
</tr>
</tbody>
</table>
### List Type | Description | Command
---|---|---
VPN | List of one or more VPNs in the overlay network. To configure multiple VPNs in a single list, include multiple `vpn` options, specifying one VPN number in each option. You can specify a single VPN identifier (such as `vpn 1`) or a range of VPN identifiers (such as `vpn 1-10`). | `vpn-list list-name`<br>`vpn vpn-id`<br>

#### Logging Frequency

If you configure a logging action, by default, the Cisco vEdge device logs all data packet headers to a syslog file. To log only a sample of the data packet headers:

```bash
vEdge(config)# policy log-frequency number
```

`number` specifies how often to log packet headers. For example, if you configure `log-frequency 20`, every sixteenth packet is logged. While you can configure any integer value for the frequency, the software rounds the value down to the nearest power of 2.

#### Cflowd Templates

For each cflowd data policy, you must create a template that defines the location of the flow collector:

```bash
vSmart(config)# policy cflowd-template template-name
```

The template can specify cflowd parameters or it can be empty. With no parameters, the data flow cache on routers is managed using default settings, and no flow export occurs.

In the cflowd template, you can define the location of the flow collection:

```bash
vSmart(config-cflowd-template-template-name)# collector vpn vpn-id address ip-address port port-number transport transport-type source-interface interface-name
```

You can configure one cflowd template per Cisco device, and it can export to a maximum of four collectors.

You can configure flow export timers:

```bash
vSmart(config)# policy cflowd-template template-name
vSmart(config-cflowd-template-template-name)# flow-active-timeout seconds
vSmart(config-cflowd-template-template-name)# flow-inactive-timeout seconds
vSmart(config-cflowd-template-template-name)# template-refresh seconds
```

By default, an actively flowing data set is exported to the collector every 600 seconds (10 minutes), a data set for a flow on which no traffic is flowing is sent every 60 seconds (1 minute), and the cflowd template record fields are sent to the collector every 90 seconds. For flow sampling, by default, a new flow is started immediately after an existing flow ends.

For a single Cisco device, you can configure a maximum of four collectors.

#### Data Policy Instance

For each centralized data policy, you create a named container for that policy with a `policy data-policy policy-name` command. For a single Cisco device, you can configure a maximum of four cflowd policies.

#### VPN Lists

Each centralized data policy instance applies to the VPNs contained in a VPN list. Within the policy, you specify the VPN list with the `policy data-policy vpn-list list-name` command. The list name must be one that you created with a `policy lists vpn-list list-name` command.
Sequences

Within each VPN list, a centralized data policy contains sequences of match–action pairs. The sequences are numbered to set the order in which data traffic is analyzed by the match–action pairs in the policy. You configure sequences with the `policy data-policy vpn-list sequence` command.

Each sequence in a centralized data policy can contain one `match` command and one `action` command.

Match Parameters

Centralized data policy can match IP prefixes and fields in the IP headers. You configure the match parameters under the `policy data-policy vpn-list sequence match` command.

For data policy, you can match these parameters:

<table>
<thead>
<tr>
<th>Description</th>
<th>Command</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group of destination prefixes</td>
<td><code>destination-data-prefix-list list-name</code></td>
<td>Name of a <code>data-prefix-list</code> list.</td>
</tr>
<tr>
<td>Individual destination prefix</td>
<td><code>destination-ip prefix/length</code></td>
<td>IP prefix and prefix length</td>
</tr>
<tr>
<td>Destination port number</td>
<td><code>destination-port number</code></td>
<td>0 through 65535</td>
</tr>
<tr>
<td>DSCP value</td>
<td><code>dscp number</code></td>
<td>0 through 63</td>
</tr>
<tr>
<td>Internet Protocol number</td>
<td><code>protocol number</code></td>
<td>0 through 255</td>
</tr>
<tr>
<td>Group of source prefixes</td>
<td><code>source-data-prefix-list list-name</code></td>
<td>Name of a <code>data-prefix-list</code> list.</td>
</tr>
<tr>
<td>Individual source prefix</td>
<td><code>source-ip prefix/length</code></td>
<td>IP prefix and prefix length</td>
</tr>
<tr>
<td>Source port number</td>
<td><code>source-port address</code></td>
<td>0 through 255</td>
</tr>
</tbody>
</table>

Action Parameters

When data traffic matches the conditions in the match portion of a centralized data policy, the packet can be accepted or rejected, and you can configure a counter for the accepted or rejected packets. You configure the action parameters under the `policy data-policy vpn-list sequence action` command.

<table>
<thead>
<tr>
<th>Description</th>
<th>Command</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Count the accepted or dropped packets.</td>
<td><code>count counter-name</code></td>
<td>Name of a counter. To display counter information, use the <code>show policy access-lists counters</code> command on the Cisco device.</td>
</tr>
<tr>
<td>Enable cflowd.</td>
<td><code>cflowd</code></td>
<td>—</td>
</tr>
<tr>
<td>Description</td>
<td>Command</td>
<td>Value or Range</td>
</tr>
<tr>
<td>-------------</td>
<td>---------</td>
<td>---------------</td>
</tr>
<tr>
<td>Log the packet headers into the messages and vsyslog system logging (syslog) files. In addition to logging the packet headers, a syslog message is generated the first time a packet header is logged and then every 5 minutes thereafter, as long as the flow is active.</td>
<td>log</td>
<td>To display logging information, use the show app log flow-all, show app log flows, and show log commands on the Cisco vEdge device.</td>
</tr>
</tbody>
</table>

For a packet that is accepted, configure the parameter **cflowd** to enable packet collection.

**Default Action**

If a data packet being evaluated does not match any of the match conditions in a control policy, a default action is applied to this route. By default, the route is rejected. To modify this behavior, include the policy **data-policy vpn-list default-action accept** command.

**Apply and Enable Cflowd Policy**

For a centralized data policy to take effect, you must apply it to a list of sites in the overlay network:

```
vSmart(config)# apply-policy site-list list-name data-policy policy-name
```

To activate the cflowd template, associate it with the data policy:

```
vSmart(config)# apply-policy cflowd-template template-name
```

For all **data-policy** policies that you apply with **apply-policy** commands, the site IDs across all the site lists must be unique. That is, the site lists must not contain overlapping site IDs. An example of overlapping site IDs are those in the two site lists `site-list 1 site-id 1-100` and `site-list 2 site-id 70-130`. Here, sites 70 through 100 are in both lists. If you were to apply these two site lists to two different **data-policy** policies, the attempt to commit the configuration on the Cisco vSmart Controller would fail.

The same type of restriction also applies to the following types of policies:

- Application-aware routing policy (**app-route-policy**)
- Centralized control policy (**control-policy**)
- Centralized data policy (**data-policy**)

You can, however, have overlapping site IDs for site lists that you apply for different types of policy. For example, the sites lists for **control-policy** and **data-policy** policies can have overlapping site IDs. So for the two example site lists above, `site-list 1 site-id 1-100` and `site-list 2 site-id 70-130`, you could apply one to a control policy and the other to a data policy.

As soon as you successfully activate the configuration by issuing a **commit** command, the Cisco vSmart Controller pushes the data policy to the Cisco devices located in the specified sites. To view the policy as configured on the Cisco vSmart Controller, use the show running-config command on the Cisco vSmart Controller. To view the policy that has been pushed to the Cisco device, use the show policy from-vsmart command on the Cisco device.

To display the centralized data policy as configured on the Cisco vSmart Controller, use the **show running-config** command:
vSmart# show running-config policy
vSmart# show running-config apply-policy

Enable Cflowd Visibility on Cisco Devices

You can enable cflowd visibility directly on Cisco devices, without configuring a data policy, so that you can perform traffic flow monitoring on traffic coming to the router from all VPNs in the LAN. To do this, configure cflowd visibility on the device:

Device(config)# policy flow-visibility

To monitor the applications, use the show app cflowd flows and show app cflowd statistics commands on the Cisco device.

Cflowd Traffic Flow Monitoring Configuration Example

This topic shows a straightforward example of configuring traffic flow monitoring.

Configuration Steps

You enable cflowd traffic monitoring with a centralized data policy, so all configuration is done on a Cisco vSmart Controller. The following example procedure monitors all TCP traffic, sending it to a single collector:

1. Create a cflowd template to define the location of the collector and to modify cflowd timers:

   vsmart(config)# policy cflowd-template test-cflowd-template
   vsmart(config-cflowd-template-test-cflowd-template)# collector vpn 1 address 172.16.155.15 port 13322 transport transport_udp
   vsmart(config-cflowd-template-test-cflowd-template)# flow-inactive-timeout 60
   vsmart(config-cflowd-template-test-cflowd-template)# template-refresh 90

2. Create a list of VPNs whose traffic you want to monitor:

   vsmart(config)# policy lists vpn-list vpn_1 vpn 1

3. Create a list of sites to apply the data policy to:

   vsmart(config)# policy lists site-list cflowd-sites site-id 400,500,600

4. Configure the data policy itself:

   vsmart(config)# policy data-policy test-cflowd-policy
   vsmart(config-data-policy-test-cflowd-policy)# vpn-list vpn_1
   vsmart(config-vpn-list-vpn_1)# sequence 1
   vsmart(config-sequence-1)# match protocol 6
   vsmart(config-match)# exit
   vsmart(config-sequence-1)# action accept cflowd
   vsmart(config-action)# exit
   vsmart(config-sequence-1)# exit
   vsmart(config-vpn-list-vpn_1)# default-action accept

5. Apply the policy and the cflowd template to sites in the overlay network:

   vsmart(config)# apply-policy site-list cflowd-sites data-policy test-cflowd-policy
   Device(config-site-list-cflowd-sites)# cflowd-template test-cflowd-template

6. Activate the data policy:

   vsmart(config-site-list-cflowd-sites)# validate
   Validation complete
vsmart(config-site-list-cflowd-sites)# commit
Commit complete.
vsmart(config-site-list-cflowd-sites)# exit configuration-mode

Full Example Configuration

Here is what the full example cflowd configuration looks like:

vsmart(config)# show configuration
apply-policy
  site-list cflowd-sites
    data-policy test-cflowd-policy
    cflowd-template test-cflowd-template
!
!
policy
data-policy test-cflowd-policy
  vpn-list vpn_1
    sequence 1
    match
      protocol 6
    action accept
    cflowd
!
!
default-action accept
!

cflowd-template test-cflowd-template
  flow-inactive-timeout 60
  template-refresh 90
  collector vpn 1 address 192.0.2.1 port 13322 transport transport_udp
!
lists
  vpn-list vpn_1
    vpn 1
!
site-list cflowd-sites
  site-id 400,500,600
!
!
Check the Cflowd Configuration

After you activate the cflowd configuration on the Cisco vSmart Controller, you can check it with the show running-config policy and show running-config apply-policy commands on the Cisco vSmart Controller. In addition, the configuration is immediately pushed down to the Cisco devices at the affected sites.

Check the Flows

On the Cisco devices affected by the cflowd data policy, various commands let you check the status of the cflowd flows.

To display information about the flows themselves.

vEdge# show app cflowd flows

<table>
<thead>
<tr>
<th>VPN</th>
<th>SRC IP</th>
<th>DEST IP</th>
<th>TCP PORT</th>
<th>DSCP</th>
<th>IPPROTO</th>
<th>CTRL</th>
<th>ICMP</th>
<th>CONTROL</th>
<th>EGRESS</th>
<th>INGRESS</th>
<th>TOTAL</th>
<th>TOTAL</th>
<th>MIN</th>
<th>MAX</th>
<th>TIME</th>
<th>TO EXPIRE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10.20.24.15</td>
<td>172.16.155.15</td>
<td>48772</td>
<td>13322</td>
<td>0</td>
<td>6</td>
<td>2</td>
<td>0.0.0.0</td>
<td>0</td>
<td>0</td>
<td>8</td>
<td>78</td>
<td>78</td>
<td>78</td>
<td>Wed Nov 19 12:31:45 2014</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>10.20.24.15</td>
<td>172.16.155.15</td>
<td>48773</td>
<td>13322</td>
<td>0</td>
<td>6</td>
<td>2</td>
<td>0.0.0.0</td>
<td>0</td>
<td>0</td>
<td>8</td>
<td>78</td>
<td>78</td>
<td>78</td>
<td>Wed Nov 19 12:31:50 2014</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>10.20.24.15</td>
<td>172.16.155.15</td>
<td>48774</td>
<td>13322</td>
<td>0</td>
<td>6</td>
<td>2</td>
<td>0.0.0.0</td>
<td>0</td>
<td>0</td>
<td>8</td>
<td>78</td>
<td>78</td>
<td>78</td>
<td>Wed Nov 19 12:31:55 2014</td>
<td></td>
</tr>
</tbody>
</table>
Cflowd Traffic Flow Monitoring Configuration Example

To quickly get a count of the number of flows.

```
vEdge# show app cflowd flow-count
VPN count
----------
1  12
```

To display flow statistics.

```
vEdge# show app cflowd statistics
    data_packets : 0
    template_packets : 0
    total-packets : 0
    flow-refresh : 123
    flow-ageout : 117
    flow-end-detected : 0
    flow-end-forced : 0
```

The following commands show information about the cflowd collectors and the cflowd template information that is sent to the collector.

```
vEdge# show app cflowd collector
```

```
vEdge# show app cflowd template
app cflowd template name test-cflowd-template
app cflowd template flow-active-timeout 30
app cflowd template flow-inactive-timeout 60
app cflowd template template-refresh 90
```
Cisco vEdge Device as a NAT Device

Cisco vEdge device can act as a NAT device, both on the transport side and on the service side of the router. On the transport side, the NAT functionality allows traffic from a local site to flow directly to the Internet rather than being backhauled to a colo facility that provides NAT services for Internet access. The NAT function is performed as the traffic enters the overlay tunnel to the WAN transport. On the service side, NAT functionality allows traffic from the local site to traverse the NAT before entering the overlay tunnel.

Table 37: Feature History

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco SD-WAN 19.1</td>
<td>Feature introduced. Cisco vEdge device can act as a NAT device, both on the transport side and on the service side of the router. On the transport side, the NAT functionality allows traffic from a local site to flow directly to the Internet rather than being backhauled to a colo facility that provides NAT services for Internet access.</td>
</tr>
</tbody>
</table>

- Cisco vEdge Device as a NAT Device on the Transport Side, on page 219
- Cisco vEdge Device as a Service-Side NAT Device, on page 222
- Configure Local Internet Exit, on page 223
- Configure Service-Side NAT, on page 227
- Configure Split DNS, on page 234
- Configure Transport-Side NAT, on page 244
- Service-Side NAT Configuration Example, on page 246

Cisco vEdge Device as a NAT Device on the Transport Side

To provide users at a local site with direct, secure access to Internet resources, such as websites, you can configure the Cisco vEdge device to function as a Network Address Translation (NAT) device, performing both address and port translation (NAPT). Enabling NAT allows traffic exiting from a Cisco vEdge device to pass directly to the Internet rather than being backhauled to a colocation facility that provides NAT services for Internet access. Using NAT in this way on a Cisco vEdge device can eliminate traffic “tromboning” and allows for efficient routes, that have shorter distances, between users at the local site and the network-based applications that they use.

The figure below shows the router acting as a NAT device. The vEdge splits its traffic into two flows, which you can think of as two separate tunnels. One traffic flow, shown in green, remains within the overlay network and travels between the two routers in the usual fashion, on the secure IPsec tunnels that form the overlay...
network. The second traffic stream, shown in grey, is redirected through the Cisco vEdge device’s NAT device and then out of the overlay network to a public network.

The NAT functionality on a Cisco vEdge device operates in a standard end-point independent fashion. The NAT software performs both address and port translation (NAPT). It establishes a translation entry between a private address and port pair inside the overlay network and a public address and port outside the overlay network. Once this translation entry is created, the NAT software allows incoming connections from an external host to be established with that private address and port only if that private address and port already established a connection to the external host. That is, an external host can reply to traffic from the private address and port; it cannot initiate a connection.

The Cisco SD-WAN NAT software supports 64,000 NAT flows.

**Note**
Cisco vEdge device provides Application Layer Gateway (ALG) FTP support with Network Address Translation – Direct Internet Access (NAT-DIA), Service NAT, and Enterprise Firewall.

**Transport-Side NAT Operation**

The following figure explains how the NAT functionality on the Cisco vEdge device splits traffic into two flows (or two tunnels), so that some of it remains within the overlay network and some goes directly to the Internet or other public network.
In this figure, the Cisco vEdge device has two interfaces:

- Interface ge0/1 faces the local site and is in VPN 1. Its IP address is 10.1.12.0/24.
- Interface ge0/0 faces the transport cloud and is in VPN 0 (the transport VPN). Its IP address is 192.23.100.0/24, and it uses the default OMP port number, 12346, for overlay network tunnels.

To configure the Cisco vEdge device to act as a NAT device so that some traffic from the router can go directly to a public network, you do three things:

- Enable NAT in the transport VPN (VPN 0) on the WAN-transport-facing interface, which here is ge0/0. All traffic exiting from the Cisco vEdge device, going either to other overlay network sites or to a public network, passes through this interface.
- To direct data traffic from other VPNs to exit from the Cisco vEdge device directly to a public network, enable NAT in those VPNs or ensure that those VPNs have a route to VPN 0.
- On the vCisco vSmart Controller, create a centralized data policy that redirects the desired data traffic from the non-transport VPN to VPN 0, and then apply that data policy to the non-transport VPN. In this case, we apply the policy to VPN 1.

Once NAT is enabled on the Cisco vEdge device, data traffic affected by the centralized data policy (here, the data traffic from VPN 1) is split into two flows:

- Traffic destined for another Cisco vEdge device in the overlay network remains in VPN 1, and it travels directly through the IPsec data plane tunnel from the source Cisco vEdge device to the destination Cisco vEdge device. This traffic never passes through VPN 0, and therefore it is never touched by NAT.
- Traffic destined for the public network passes from VPN 1 to VPN 0, where it is NATed. During the NAT processing, the source IP address is changed from 10.1.12.0/24 to that of ge0/0, 179.23.100.0/24, and the source port is changed to 1024.

When NAT is enabled, all traffic that passes through VPN 0 is NATed. This includes both the data traffic from VPN 1 that is destined for a public network, and all control traffic, including the traffic required to establish and maintain DTLS control plane tunnels between the Cisco vEdge device and the Cisco vSmart Controller and between the router and the Cisco vBond Orchestrator.
The Cisco vBond Orchestrator learns both the public and private addresses of the Cisco vEdge device, and it advertises both address to the Cisco vSmart Controller. In turn, the Cisco vSmart Controller advertises both addresses to all the devices in its domain. Each Cisco vEdge device then decides whether to use the public or the private address to communicate with another Cisco vEdge device as follows:

- If the Cisco vEdge device is located at the same site as the other router (that is, if they are both configured with the same overlay network site ID), it communicates using the private address. Because both routers have the same site ID, they are behind the same NAT, and so their communication channels are already secure.

- If the Cisco vEdge device is located at a different site, it communicates with the other router using the public address. Then, the NAT functionality on the Cisco vEdge device translates the public address to the proper private address.

If a Cisco vSmart Controller connected to a corporate NAT and a NAT-enabled Cisco vEdge device are located at the same physical overlay network site, you must configure them with different Cisco SD-WAN site identifiers in order for them to be able to communicate. Similarly, if more than one NAT-enabled Cisco vEdge device is located at the same physical overlay network site, each one must be configured with a different site identifier.

**Cisco vEdge Device as a Service-Side NAT Device**

On a Cisco vEdge device, you can configure NAT on the service side of the router so that data traffic traverses the NAT before entering the overlay tunnel that is located in the transport VPN. The service-side NAT performs NAT to mask the IP address of data traffic it receives. You can configure both dynamic NAT and 1:1 static NAT on the Cisco vEdge device.

**Service-Side NAT Operation**

The following figure explains how the Cisco vEdge device provides NAT services on the service side:

![Service-Side NAT Operation Diagram](386851)

In this figure, the Cisco vEdge device has one NAT interface in VPN 1. This interface pools all service-side traffic destined for the NAT interface. The interface name is natpool2, and its IP address is 192.168.10.1. This IP address is the address each packet's IP address is translated to.

To configure the service-side NAT operation on the Cisco vEdge device so that traffic traverses the NAT in VPN 1 before being placed on the transport tunnel towards its destination, you do two things:

- Create a NAT pool interface in VPN 1, the service-side VPN. Here, the NAT pool number is 2.

- To direct data traffic from prefixes within VPN 1 to the service-side NAT, create a centralized data policy on the vSmart controller. In the match condition, specify the prefixes to be NATed. In the action condition,
set the desired NAT pool, here, natpool 2. Then apply the data policy to the desired site (here, site 500), and apply it to traffic coming from the service side.

When service-side NAT is enabled, all matching prefixes in VPN 1 are directed to the natpool2 interface. This traffic is NATed, with the NAT swapping out the service-side IP address and replacing it with its NAT pool IP address. The packet then gets forwarded to its destination, here the data center.

Configure Local Internet Exit

To configure a Cisco vEdge device to be an Internet exit point, you enable NAT within a VPN on the Cisco vEdge device, and then you configure a centralized data policy on a Cisco vSmart controller. This policy splits the traffic within the VPN so that some of it is directed towards remote sites within the VPN, and hence remains within the overlay network, and other traffic is directed to the Internet or other destinations outside the overlay network. It is also possible to configure a Cisco vEdge device to forward data traffic directly to the Internet, by specifying the destination IP prefix.

NAT Configuration Considerations

When configuring a Cisco vEdge device to act as a NAT device, keep the following considerations in mind:

• For a Cisco vEdge device that is acting as a vBond orchestrator, do not enable NAT operation on the interface that is tied to the vBond orchestrator's IP address. If you do so, the orchestrator is placed into a private address space behind the NAT. For the overlay network to function properly, the vBond orchestrator must be in a public address space. You can, however, enable NAT operation on other Cisco vEdge device interfaces.

• When you enable NAT on a Cisco vEdge device, the router NATs all traffic that is sent out through VPN 0. That is, both data traffic and control traffic are NATed.

• The NAT operation on outgoing traffic is performed in VPN 0, which is always only a transport VPN. The router's connection to the Internet is in VPN 0. Performing the NAT operation in VPN 0 avoids the IPSec tunnels that carry data traffic within the overlay network.

• If you configure NAT on multiple interfaces in VPN 0, ECMP is performed among the interfaces.

• When you use NAT—either by configuring it on an interface or by setting it as an action in a centralized data policy—no route lookup is performed. Instead, traffic is forwarded to one of the available NAT default gateways.

• The Cisco vEdge device NAT implementation uses end-point–independent NAT. If your network contains other NAT devices that interact with the Cisco vEdge device NAT, these devices must either perform end-point–independent NAT, or they must be configured with policy rules so that they do not change the port numbers for Cisco SD-WAN overlay network destinations.

• When a Cisco vEdge device has two or more NAT interfaces, and hence two or more DIA connections to the internet, by default, data traffic is forwarding on the NAT interfaces using ECMP. To direct data traffic to a specific DIA interface, configure a centralized data policy on the Cisco vSmart controller that sets two actions—nat and local-tloc color. In the local-tloc color action, specify the color of the TLOC that connects to the desired DIA connection.

• Interface IP has to be lesser than NAT range start IP. It is required for IP address of the NAT interface to be lower than the IP addresses used for the IP NAT pool range and static NAT translations. When this requirement is not met, the error is displayed and the configuration will be rejected. When NAT interface
IP is higher than the static NAT mapping IP entry, error "Source address is not in the range of the interface IP prefix" displays. The address assigned to the interface IP is in the same subnet as the static mapping IP.

For example, interface IP is 192.168.1.100/24, and the natpool has a range of 192.168.1.10 to 192.168.1.30 with a static mapping of the translated address 192.168.1.10, configuration will be rejected, error will displayed.

If the interface IP is lower than the natpool range and static mapping, it allows to commit the configuration with no issues, configuration will be accepted.

For example, interface IP is 192.168.1.1, and the natpool has a range of 192.168.1.10 to 192.168.1.30 with a static mapping of the translated address 192.168.1.10, configuration will be accepted as the interface IP is lower than the natpool range and static mapping, it allows to commit the configuration with no issues.

Direct Traffic to Exit to the Internet Using Data Policy

To use a centralized data policy to direct traffic from a Cisco vEdge device directly to the Internet, you enable NAT functionality in the WAN VPN or VPNs, and then you create and apply a centralized data policy.

Enable NAT Functionality in the WAN VPN

The first step in setting up Internet exit on a Cisco vEdge device is to configure the router to act as a NAT device. You do this by enabling NAT functionality in VPNs that have interfaces that connect to a WAN transport network. By default, VPN 0 always connects to the WAN transport. Other VPNs in your network might also connect to WANs.

To configure a Cisco vEdge device to act as a NAT device:

1. Enable NAT in the desired VPN:

   vEdge(config)# vpn vpn-id  interface interface-name nat

2. By default, NAT mappings from the Cisco SD-WAN overlay network side of the NAT to the external side of the NAT remain active, and NAT mapping timers are refreshed regularly to keep the mapping operational. To also refresh NAT mappings of packets coming from the external side of the NAT into the overlay network, change the refresh behavior:

   vEdge(config-nat)# refresh bi-directional

3. NAT sessions time out after a period of non-use. By default, TCP sessions time out after 60 minutes, and UDP sessions time out after 20 minutes. To change these times:

   vEdge(config-nat)# tcp-timeout minutes
   vEdge(config-nat)# udp-timeout minutes

   The times can be from 1 to 65535 minutes.

   The following NAT session timers are fixed, and you cannot modify them:

   • TCP session timeout if no SYN-ACK response is received—5 seconds
   • TCP session timeout if three-way handshaking is not established—10 seconds
   • TCP session timeout after receiving a FIN/RST packet—30 seconds
   • ICMP timeout—6 seconds
   • Other IP timeout—60 seconds
4. By default, the Cisco vEdge device does not receive inbound ICMP error messages. However, NAT uses ICMP to relay error messages across a NAT. To have the router receive the NAT ICMP messages:

```
 vEdge(config-nat)# no block-icmp-error
```

In case of a DDoS attack, you might want to return to the default, to again prevent the Cisco vEdge device from receiving inbound ICMP error messages.

Create a Data Policy to Direct Traffic to the Internet Exit

To direct data traffic from a Cisco vEdge device to an Internet exit point, you split the destination of the traffic within a VPN, sending some to remote sites in the VPN and directing the traffic that is destined to the Internet (or other destinations outside the overlay network) to exit directly from the local Cisco vEdge device to the external destination.

To split the traffic, configure a centralized data policy on a Cisco vSmart controller:

1. Configure the source prefix of the data traffic:

```
 vSmart(config)# policy data-policy policy-name
 vSmart(data-policy)# vpn-list list-name
 vSmart(vpn-list)# sequence number
 vSmart(sequence)# match source-ip ip-prefix
```

2. Configure the destination of the data traffic, either by IP prefix or by port number:

```
 vSmart(sequence)# match destination-ip ip-prefix
 vSmart(sequence)# match destination-port port-number
```

3. Direct matching data traffic to the NAT functionality. You can optionally configure a packet counter.

```
 vSmart(sequence)# action accept
 vSmart(accept)# count counter-name
 vSmart(accept)# nat use-vpn 0
```

4. Configure additional sequences, as needed, for other source prefixes and destination prefixes or ports, and for other VPNs.

5. Change the default data policy accept default action from reject to accept. With this configuration, all non-matching data traffic is forwarded to service-side VPNS at remote sites instead of being dropped.

```
 vSmart(vpn-list)# default-action accept
```

6. Apply the data policy to particular sites in the overlay network:

```
 vSmart(config)# apply-policy site-list list-name data-policy policy-name from-service
```

Direct Traffic To Exit to the Internet Based Only on IP Prefix

You can direct local data traffic to exit to the internet based only on the destination IP prefix. To configure this, in the service VPN, forward traffic that is destined towards an internet location to VPN 0, which is the WAN transport VPN:

```
 vEdge(config)# vpn vpn-id
 vEdge(config-vpn)# ip route prefix vpn 0
```

In the `vpn` command, specify the VPN ID of the service-side VPN from which you are sending the traffic. In the `ip route` command, `prefix` is the IPv4 prefix of the remote destination. The `vpn 0` option configures the software to perform the route lookup in VPN 0 rather than in the service-side VPN. This is done because the service-side VPN cannot resolve the route.
For the traffic redirection to work, in VPN 0, you must enable NAT on the interface associated with the configured prefix:

```
vedge(config)# vpn 0 interface interface-name nat
```

Here, the interface is the one to use to reach the destination prefix.

The following snippet illustrates the two parts of the configuration:

```
vEdge# show running-config vpn 1
vpn 1
...
ip route 10.1.17.15/32 vpn 0
!
vEdge# show running-config vpn 0
vpn 0
...
interface ge0/1
...
nat
!
no shutdown
!
```

To verify that the redirection is working properly, look at the output of the `show ip routes` command:

```
vEdge# show ip routes
Codes Protos-Protosub-type:  
IA -> ospf-inter-area,  
E1 -> ospf-external1, E2 -> ospf-external2,  
N1 -> ospf-nssa-external1, N2 -> ospf-nssa-external2,  
* -> bgp-external, i -> bgp-internal
Codes Status flags:  
F -> fib, S -> selected, I -> inactive,  
B -> blackhole, R -> recursive

VRF PREFIX PROTOCOL SUB TYPE IP NAME ADDR VPN TLOC IP COLOR ENCAP STATUS
----------------------------------------------------------------------------------------------------------------------------------
0 0.0.0.0/0 static  -  ge0/0 10.1.15.13 - - - - F,S
0 10.0.0.0/24 connected -  ge0/3 - - - - - F,S
0 10.0.100.0/24 connected -  ge0/7 - - - - - F,S
0 10.1.15.0/24 connected -  ge0/1 - - - - - F,S
0 10.1.17.0/24 connected -  ge0/1 - - - - - F,S
0 10.1.17.0/24 ospf -  ge0/1 - - - - - -
0 57.0.2.0/24 connected -  system - - - - - F,S
0 172.16.255.12/32 connected -  system - - - - - F,S
1 10.1.17.15/32 nat  -  ge0/1 - - - - - F,S
0 10.20.24.0/24 ospf -  ge0/1 - - - - - -
1 10.20.24.0/24 connected -  ge0/4 - - - - - -
1 10.20.24.0/24 ospf -  ge0/1 - - - - - -
1 55.0.1.0/24 connected -  ge0/5 - - - - - -
1 55.0.1.0/24 ospf -  ge0/5 - - - - - -
1 60.0.1.0/24 ospf -  ge0/1 - - - - - -
1 61.0.1.0/24 connected -  system - - - - - F,S
512 10.0.1.0/24 connected -  system - - - - - F,S
```

In VPN 1, the prefix 10.1.17.15/32 is associated with the protocol "nat", which reflects the configuration of the `ip route` command in VPN 1. For this prefix, the next-hop interface is `ge0/1`, and the next-hop VPN is VPN 0. This prefix is installed into the route table only if the resolving next hop is over an interface on which NAT is enabled.

The prefix that you configure in the `ip route` represents a route in the specified VPN (the service VPN whose ID you enter in the first command above). To direct traffic to that prefix, you can redistribute it into BGP or OSPF:

```
vedge(config-vpn)# bgp address-family address-family redistribute nat
vedge(config-vpn)# ospf redistribute nat
```

### Track Transport Interface Status

When you enable NAT on a transport interface to allow the local router to forward traffic directly to the internet rather than first forwarding the traffic to a data center router connected to the internet, the router directs data traffic according to the centralized data policy that is applied to that interface, forwarding some
traffic directly to the internet (or other external network) and other traffic to other VPNs in the overlay network, including the data center. If the internet or external network becomes unavailable, for example, due to a brownout, the router has no way to learn of this disruption, and it continues to forward traffic based on the policy rules. The result is that traffic that is being forwarded to the internet is silently dropped.

To prevent the internet-bound traffic from being dropped, you can configure the router to track the status of the transport interface and to redirect the traffic to the non-NATed tunnel on the transport interface when the local internet is unavailable. With tracking enabled, the router periodically probes the path to the internet to determine whether it is up. When it detects that the path is down, the router withdraws the NAT route to the internet destination, and reroutes the traffic to the non-NATed tunnel on the interface so that another router in the overlay network can forward the traffic to the internet. The local router continues to periodically check the status of the path to the interface. When it detects that the path is again functioning, the router reinstalls the NAT route to the internet.

To track the transport interface status, you create a global interface tracker, and then you apply it to the transport interface on which NAT is enabled.

To create a transport interface tracker:

```bash
vEdge(config)# system
vEdge(config-system)# tracker tracker-name
vEdge(config-tracker)# endpoint-dns-name dns-name
vEdge(config-tracker)# endpoint-ip ip-address
vEdge(config-tracker)# interval seconds
vEdge(config-tracker)# multiplier number
vEdge(config-tracker)# threshold milliseconds
```

The tracker name can be up to 128 lowercase characters.

At a minimum, you must specify the IP address or DNS name of a destination on the internet. This is the destination to which the router sends probes to determine the status of the transport interface. You can configure either one IP address or one DNS name.

By default, a status probe is sent every minute (60 seconds). To modify this value, change the time in the `interval` command to a value from 10 through 600 seconds.

By default, the router waits 300 milliseconds to receive a response from the internet destination. To modify the time to wait for a response, change the time in the `threshold` command to a value from 100 through 1000 milliseconds.

By default, after sending three probes and receiving no responses, the router declares that transport interface is down. To modify the number of retries, change the number in the `multiplier` command to a value from 1 through 10.

You can configure up to eight interface trackers.

To apply a tracker to a transport interface:

```bash
vEdge(config)# vpn 0
vEdge(vpn)# interface interface-name
vEdge(interface)# tracker tracker-name
```

You can apply only one tracker to an interface.

---

**Configure Service-Side NAT**

You can configure both dynamic NAT and 1:1 static NAT on the service side of a router. To do so, you create a NAT pool interface within a service VPN on the router, and then you configure a centralized data policy on
the Cisco vSmart controller. This policy directs data traffic with the desired prefixes to the service-side NAT. Finally, you configure either dynamic NAT or static NAT on the desired NAT pool interfaces.

**Create a NAT Pool Interface**

On the router, you create a NAT pool interface. This interface NATs data traffic that is directed to it and then forwards the traffic towards its destination.

To create a NAT pool interface:

1. In the desired VPN, create the NAT pool interface:

   ```
   vEdge(config-vpn)# interface natpool number
   ```

   The pool can have a number from 1 through 31. You refer to this NAT pool number in the action portion of the centralized data policy that you configure to direct data traffic to the pool. You can configure a maximum of 31 NAT pool interfaces in a VPN.

2. Configure the NAT pool interface’s IP address:

   ```
   vEdge(config-natpool)# ip address prefix/show ip routes length
   ```

   The length of the IP address determines the number of addresses that the router can NAT at the same time. For each NAT pool interface, you can configure a maximum of 250 IP addresses.

3. Enable the interface:

   ```
   vEdge(config-natpool)# no shutdown
   ```

   On a NAT pool interface, you can configure only these two commands (ip address and shutdown/no shutdown) and the nat command, discussed below. You cannot configure any of the other interface commands.

Here is an example of configuring the NAT pool interface:

```
vEdge# show running-config vpn 1
vpn 1
 interface ge0/4
   ip address 10.20.24.15/24
   no shutdown
 !
 interface ge0/5
   ip address 56.0.1.15/24
   no shutdown
 !
 interface natpool2
   ip address 192.179.10.1/32
   nat
 !
 !
```

To display information about the NAT pool interface, use the `show interface` command:

```
vEdge# show interface vpn 1
```

To display information about the NAT pool interface, use the `show interface` command:
Create a Data Policy To Direct Data Traffic to a Service-Side NAT

To direct data traffic from the service side of the router to the NAT, you create a centralized data policy on the Cisco vSmart controller. In the match condition of the policy, you identify the data traffic that you want to direct to the NAT. One way to do this is to match on the IP prefixes of the data traffic. In the action condition of the policy, you direct the matching traffic to one of the number NAT pools. Finally, you apply the policy to the service side at the desired overlay network sites.

To create a data policy to direct data traffic to a service-side NAT:

1. Configure the lists required for the data policy. You must configure a list of VPN and sites. If you are matching on data prefixes, configure a data prefix list.

   ```
   vSmart(config-policy-lists)# vpn-list list-name
   vSmart(config-policy-vpn-list)# vpn vpn-id
   vSmart(config-policy-lists)# site-list list-name
   vSmart(config-policy-site-list)# site-id site-id
   vSmart(config-policy-lists)# data-prefix-list list-name
   vSmart(config-policy-data-prefix-list)# ip-prefix prefix/length
   ```

2. Configure a data policy:

   ```
   vSmart(config-policy)# data-policy policy-name
   vSmart(config-data-policy)# vpn-list list-name
   vSmart(config-vpn-list)# sequence number
   ```

3. Configure the desired match conditions:

   ```
   vSmart(config-sequence)# match condition
   ```

4. In the action, associate matching data traffic with the desired NAT pool:

   ```
   vSmart(config-sequence)# action accept
   vSmart(config-sequence)# nat pool number
   ```

5. Configure the desired default action for the data policy:

   ```
   vSmart(config-vpn-list)# default-action (accept | reject)
   ```

6. Apply the policy to the desired sites in the overlay network:

   ```
   vSmart(config)# apply-policy site-list list-name data-policy policy-name from-service
   ```

Here is an example of configuring the centralized data policy:

```
vSmart# show running-config policy
data-policy service-side-nat-policy
   vpn-list vpn-1
   sequence 10
   match
   source-data-prefix-list prefixes-to-nat
   action accept
   nat pool 2
!
default-action accept
!
lists
vpn-list vpn-1
vpn 1
!
data-prefix-list prefixes-to-nat
```
ip-prefix 56.0.1.0/24
!
site-list site-500
  site-id 500
!
!
vSmart# show running-config apply-policy
apply-policy
  site-list site-500
  data-policy service-side-nat-policy from-service
!
!
After you activate the policy, you can see that it has been applied to the router:

vEdge# show policy from-vsmart
from-vsmart data-policy service-side-nat-policy
direction from-service
  vpn-list vpn-1
  sequence 10
  match
    source-data-prefix-list prefixes-to-nat
  action accept
    nat pool 2
  default-action accept
  from-vsmart lists vpn-list vpn-1
  vpn 1
from-vsmart lists data-prefix-list prefixes-to-nat
  ip-prefix 56.0.1.0/24

Configure Dynamic NAT

By default, when you configure a router to act as a NAT, the router performs dynamic network address translation. In this capacity, the router can perform dynamic NAT for up to 250 IP addresses across NAT pools.

To configure dynamic NAT:

1. In the desired VPN, create the NAT pool interface:

   vEdge(config-vpn)# interface natpool number

   The pool can have a number from 1 through 31. You refer to this NAT pool number in the action portion of the centralized data policy that you configure to direct data traffic to the pool. You can configure a maximum of 31 NAT pool interfaces in a VPN.

2. Configure the IP address prefix for the NAT pool interface:

   vEdge(config-natpool)# ip address prefix/length

   The prefix length determines the maximum number of addresses that the router can NAT at the same time. For example, for a /30 prefix length, the router can perform translation on four addresses at a time. For each NAT pool interface, you can configure a maximum of 250 IP addresses.

3. Enable the interface:

   vEdge(config-natpool)# no shutdown

4. Enable dynamic NAT:

   vEdge(config-natpool)# nat
As mentioned above, the length of the IP address determines the number of IP addresses that the router can NAT at the same time, up to a maximum of 250 across all NAT pools. When all available IP addresses have been used, the router reuses the last IP address multiple times, changing the port number. The port number is chosen at random from the nonreserved port numbers, that is, those port numbers in the range 1024 through 65535. For example, if the IP address is 10.1.17.30, the Cisco vEdge device can uniquely NAT four IP addresses. Let us say that the router maps the fourth IP address to 10.1.20.5, or more specifically to 10.1.20.5:12346 if we include the port number. It would then map the fifth IP address to the same IP address, but with a different port, such as 10.1.20.5:12347. To have the router drop packets when no more IP addresses are available for the translation process, include the following command:

```
vEdge(config)# vpn vpn-id interface natpool number
vEdge(config-natpool)# no overload
```

**Configure Static NAT**

You can configure a router acting as a NAT to perform static network address translation (also called 1:1 static NAT) of source IP addresses. You can translate service-side source addresses before sending packets out to the overlay network, and you can translate external addresses before forwarding packets to the service-side network. You can also translate service-side source addresses before sending packets out to another service-side LAN connected to the same router.

For packets originating on the service side of a router, you can statically map the packets' source IP address to another IP address. You do this by creating a NAT pool interface within a service-side VPN. For this interface, you configure a pool of IP addresses to use for network address translation, and then you configure the static address mappings. When the address pool is depleted, you can choose to drop packets that have unmapped source IP addresses. Dropping these packets is not the default behavior.

For packets exiting a transport tunnel from a router, you can statically map the packet's source IP address to another IP address, generally to an address that is routable within the service-side network. You configure this in the same way as for NATing packets originating on the service side.

You must create separate NAT pool interfaces to translate source IP addresses for service-side packets and for tunnel packets.

Across all NAT pools, a vEdge router can NAT a maximum of 254 source IP addresses. This is the number of addresses in a /24 prefix, less the .0 and .255 addresses. You cannot configure translation for .0 and .255 addresses.

This section explains how to configure static NAT for translating service-side source IP addresses and for translating external (transport-side) IP addresses. The two procedures are very similar, but we describe them separately for clarity.

**Static NATing of Service-Side Addresses**

To configure the static NATing of service-side source IP addresses:

1. In the desired VPN, create the NAT pool interface:

   ```
vEdge(config-vpn)# interface natpool number
   ```

   The pool can have a number from 1 through 31. You refer to this NAT pool number in the action portion of the centralized data policy that you configure to direct data traffic to the pool. You can configure a maximum of 31 NAT pool interfaces in a VPN.

2. Enable the NAT pool interface:

   ```
vEdge(config-natpool)# no shutdown
   ```
3. Configure the IP address prefix for the NAT pool interface

   vEdge(config-natpool)# ip address prefix/length

   The prefix length determines the maximum number of source IP addresses that can be NATed in the NAT pool. For example, for a /30 prefix length, a maximum of four source IP addresses can be NATed. For each NAT pool interface, you can configure a maximum of 250 IP addresses.

4. Configure the NAT pool interface to perform network address translation:

   vEdge(config-natpool)# nat

5. By default, all IP addresses are translated to an address in the pool of NAT addresses configured in the ip address command. The addresses are mapped one to one until the address pool is depleted. Then, the first address is used multiple times, and the port number is changed to a random value between 1024 and 65535. This reuse of the last address is called overloading. Overloading effectively implements dynamic NAT.

   To configure static NAT, include the no overload command to enforce the mapping of a single source IP address to a single translated IP address:

   vEdge(config-nat)# no overload

   With this command, when the maximum number of available IP addresses available to be translated is reached, packets with other IP addresses are dropped.

6. Set the direction in which the NAT pool interface performs static mapping to inside to statically translate service-side IP source addresses:

   vEdge(config-nat)# direction inside

   Note that the default direction is inside.

   A single NAT pool interface can perform static address translation either for service-side source addresses (direction inside) or for external source addresses (direction outside), but not for both. This means that for a single NAT pool, you can configure only one direction command.

7. Define the static address translations for service-side source IP addresses:

   vEdge(config-nat)# static source-ip ip-address1 translate-ip ip-address2 inside

   ip-address1 is the source IP address of a device or branch router on the service side of the Cisco vEdge device.

   ip-address2 is the translated source IP address. This is the address that the Cisco vEdge device places in the source field of the packet's IP header when transmitting the packet out the transport network. Because the NAT pool direction is inside, this IP address must be in the interface's IP address range. This is the IP address prefix configured in the ip address command.

   The inside option indicates that it is a service-side, or inside, address that is being statically translated. Note that the inside option in the static command is different from and independent of the inside or outside option you specify in the direction command. When you are statically NATing service-side addresses, you can statically map both service-side addresses (with a static...inside command) and transport-side addresses (with a static...outside command), as described in the next step. The maximum number of service-side source IP addresses that you can statically NAT is equal to the number of addresses available in the interface's prefix range. For example, for a /30 prefix length, you can configure a maximum of four static NAT mappings.

   Once the NAT static address mapping is installed in the router's NAT table, the router can perform source IP address translation in both directions—when a service-side packet is being transmitted into the transport network, and when an external packet (addressed to ip-address2) arrives at the router.
8. Define the static address translations for transport-side source IP addresses:

vEdge(config-nat)# static source-ip ip-address1 translate-ip ip-address2 outside

ip-address1 is the source IP address of an external device or router, that is, of a device at a remote site.

ip-address2 is the translated source IP address. This is the address that the vEdge router places in the source field of the packet's IP header before forwarding the traffic to the service-side network.

The outside option indicates that an external IP address is being statically translated. Note that the outside option in the static command is different from and independent of the inside or outside option you specify in the direction command. When you are statically NATing service-side addresses, you can statically map both service-side addresses (with a static...inside command) and transport-side addresses (with a static...outside command), as described in the previous step.

Because the direction of the NAT pool is inside, the pool of IP addresses set aside for NATing is used only to NAT service-side source IP addresses. This means that here, you can configure any number of external static address translations.

As a corollary of NATing an external IP address, when a service-side device responds to that external IP address, it simply takes the source IP address from the received packet and places it into the destination IP field in the IP header.

9. Optionally, log the creation and deletion of NAT flows:

vEdge(config-nat)# log-translations

**Static NATing of External Addresses**

To configure the static NATing of external source IP addresses:

1. In the desired VPN, create the NAT pool interface:

vEdge(config-vpn)# interface natpool number

The pool can have a number from 1 through 31. You refer to this NAT pool number in the action portion of the centralized data policy that you configure to direct data traffic to the pool. You can configure a maximum of 31 NAT pool interfaces in a VPN.

2. Enable the NAT pool interface:

vEdge(config-natpool)# no shutdown

3. Configure the IP address prefix for the NAT pool interface:

vEdge(config-natpool)# ip address prefix/length

The prefix length determines the maximum number of IP addresses that the router can NAT at the same time in that NAT pool. For example, for a /30 prefix length, the router can perform translation on four addresses at a time. For each NAT pool interface, you can configure a maximum of 250 IP addresses.

4. Configure the NAT pool interface to perform network address translation:

vEdge(config-natpool)# nat

5. By default, all IP addresses are translated to an address in the pool of NAT addresses configured in the ip address command. The addresses are mapped one to one until the address pool is depleted. Then, the last address is used multiple times, and the port number is changed to a random value between 1024 and 65535. This reuse of the last address is called overloading. Overloading effectively implements dynamic NAT. To configure static NATing of external addresses, you must include the no overload command to...
enforce the mapping of a single source IP address to a single translated IP address, because the software does not support overloading on the outside NAT pool interface:

```plaintext
vEdge(config-nat)# no overload
```

With this command, when the maximum number of available IP addresses available to be translated is reached, packets with other IP addresses are dropped.

6. Set the direction in which the NAT pool interface performs static mapping to `outside` to statically translate external IP source addresses:

```plaintext
vEdge(config-nat)# direction outside
```

The default direction is `inside`.

A single NAT pool interface can perform static address translation either for service-side source addresses (`direction inside`) or for external source addresses (`direction outside`), but not for both. This means that for a single NAT pool, you can configure only one `direction` command.

7. Define the static address translations for external source-IP addresses:

```plaintext
vEdge(config-nat)# static source-ip ip-address1 translate-ip ip-address2 outside
```

`ip-address1` is the source IP address of a remote device or router on the transport side of the router.

`ip-address2` is the translated source IP address. This is the address that the router places in the source field of the packet's IP header when forwarding the packet into the service-side network. Because the NAT pool direction is `outside`, this IP address must be in the interface's IP address range. This is the IP address prefix configured in the `ip address` command.

The `outside` option indicates that it is an external, or outside, address that is being statically translated. Note that the `outside` option in the `static` command is different from and independent of the `inside` or `outside` option you specify in the `direction` command. When you are statically NATing external addresses, you can statically map both transport-side addresses (with a `static...outside` command) and service-side addresses (with a `static...inside` command), as described in the previous step.

The maximum number of external source IP addresses that you can statically NAT is equal to the number of addresses available in the interface's prefix range. For example, for a /30 prefix length, you can configure a maximum of four static NAT mappings.

As a corollary of NATing an external IP address, when a service-side device responds to that external IP address, it simply takes the source IP address from the received packet and places it into the destination IP field in the IP header.

---

**Configure Split DNS**

When an application-aware routing policy allows a Cisco vEdge device to send application traffic to and receive application traffic from a service VPN, the router performs a Domain Name System (DNS) lookup to determine how to reach a server for the application. If the router does not have a connection to the internet, it sends DNS queries to a router that has such a connection, and that router determines how to reach a server for that application. In a network in which the internet-connect router is in a geographically distant data center, the resolved DNS address might point to a server that is also geographically distant from the site where the service VPN is located.

Because you can configure a Cisco vEdge device to be an internet exit point, it is possible for any router to reach the internet directly to perform DNS lookups. To do this, you create a policy that configures split DNS and that defines, on an application-by-application basis, how to perform DNS lookups.
You configure split DNS with either a centralized data policy or, if you want to apply SLA criteria to the data traffic, an application-aware routing policy. You create these policies on a Cisco vSmart controller, and they are pushed to the Cisco vEdge devices.

**CLI Configuration Procedure**

**Configure Split DNS with a Centralized Data Policy**

The following high-level steps show the minimum policy components required to enable split DNS with a centralized data policy:

1. Create one or more lists of overlay network sites to which the centralized data policy is to be applied (in an `apply-policy` command):
   ```
   vSmart(config)# policy
   vSmart(config-policy)# lists site-list list-name
   vSmart(config-lists)# site-id site-id
   ```
   The list can contain as many site IDs as necessary. Include one `site-id` command for each site ID. For contiguous site IDs, you can specify a range of numbers separated with a dash (`-`).

2. Create lists of applications or application families for which you want to enable split DNS. You refer to these lists in the `match` section of the data policy.
   ```
   vSmart(config)# policy lists
   vSmart(config-lists)# app-list list-name
   vSmart(config-app-list)# (app application-name | app-family family-name)
   ```

3. Create lists VPNs to which the split DNS policy is to be applied (in a `policy data-policy` command):
   ```
   vSmart(config)# policy lists
   vSmart(config-lists)# vpn-list list-name
   vSmart(config-lists)# vpn vpn-id
   ```

4. Create a data policy instance and associate it with a list of VPNs:
   ```
   vSmart(config)# policy data-policy policy-name
   vSmart(config-data-policy)# vpn-list list-name
   ```

5. Create a series of match–action pair sequences:
   ```
   vSmart(config-vpn-list)# sequence number
   ```
   The match–action pairs are evaluated in order, by sequence number, starting with the lowest numbered pair and ending when the route matches the conditions in one of the pairs. Or if no match occurs, the default action is taken (either rejecting the route or accepting it as is).

6. Process the DNS server resolution for the applications or application families contained in an application list. In `list-name`, specify one of the names in a `policy lists app-list` command.
   ```
   vSmart(config-sequence)# match dns-app-list list-name
   ```

7. Configure the match–action pair sequence to process DNS requests (for outbound data traffic) or responses (for inbound data traffic):
   ```
   vSmart(config-sequence)# match dns (request | response)
   ```

8. Accept matching packets, optionally counting and logging them:
   ```
   vSmart(config-sequence)# action accept [count counter-name] [log]
   ```

9. Enable local internet exit:
vSmart(config-sequence)# action accept nat [pool number] [use-vpn 0]

10. By default, the DNS servers configured in the VPN in which the policy is applied are used to process DNS lookups for the applications. You can direct DNS requests to a particular DNS server. For a data policy condition that applies to outbound traffic (from the service network), configure the IP address of the DNS server:

vSmart(config-sequence)# action accept redirect-dns ip-address

For a data policy condition that applies to inbound traffic (from the tunnel), include the following so that the DNS response can be correctly forwarded back to the service VPN:

vSmart(config-sequence)# action accept redirect-dns host

11. If a route does not match any of the conditions in one of the sequences, it is rejected by default. To accept nonmatching prefixed, configure the default action for the policy:

vSmart(config-policy-name)# default-action accept

12. Apply the policy to one or more sites in the overlay network:

vSmart(config)# apply-policy site-list list-name data-policy policy-name (all | from-service | from-tunnel)

Configure Split DNS with an Application-Aware Routing Policy

The following high-level steps show the minimum policy components required to enable split DNS with an application-aware routing policy:

1. Create one or more lists of overlay network sites to which the centralized data policy is to be applied (in an apply-policy command):

vSmart(config)# policy
vSmart(config-policy)# lists site-list list-name
vSmart(config-lists-list-name)# site-id site-id

The list can contain as many site IDs as necessary. Include one site-id command for each site ID. For contiguous site IDs, you can specify a range of numbers separated with a dash (-).

2. Create SLA classes and traffic characteristics to apply to matching application data traffic:

vSmart(config)# policy sla-class sla-class-name
vSmart(config-sla-class)# jitter milliseconds
vSmart(config-sla-class)# latency milliseconds
vSmart(config-sla-class)# loss percentage

3. Create lists of applications or application families to identify application traffic of interest in the match section of the data policy:

vSmart(config)# policy lists
vSmart(config-lists)# app-list list-name
vSmart(config-lists-app-list)# (app application-name | app-family family-name)

4. Create lists VPNs to which the split DNS policy is to be applied (in a policy data-policy command):

vSmart(config)# policy lists
vSmart(config-lists)# vpn-list list-name
vSmart(config-lists-vpn-list)# vpn vpn-id

5. If you are configuring a logging action, configure how often to log packets to syslog files:

vEdge(config)# policy log-frequency number

6. Create an application-aware routing policy instance and associate it with a list of VPNs:
vSmart(config)# policy app-route-policy policy-name
vSmart(config-data-policy-policy-name)# vpn-list list-name

7. Create a series of match–pair sequences:
   vSmart(config-vpn-list)# sequence number
   The match–action pairs are evaluated in order, by sequence number, starting with the lowest numbered pair and ending when the route matches the conditions in one of the pairs. Or if no match occurs, the default action is taken (either rejecting the route or accepting it as is).

8. Process the DNS server resolution for the applications or application families contained in an application list. In list-name, specify one of the names in a policy lists app-list command.
   vSmart(config-sequence-number)# match dns-app-list list-name

9. Configure the match–action pair sequence to process s DNS requests (for outbound data traffic) or responses (for inbound data traffic):
   vSmart(config-sequence-number)# match (request | response)

10. Define the SLA action to take if a match occurs:
   vSmart(config-sequence)# action sla-class sla-class-name [strict]
   vSmart(config-sequence)# action sla-class sla-class-name [strict] preferred-color colors
   vSmart(config-sequence)# action backup-sla-preferred-color colors

11. For matching packets, optionally count and log them:
    vSmart(config-sequence)# action count counter-name
    vSmart(config-sequence)# action log

12. Enable local internet exit:
    vSmart(config-sequence-number)# action acccept nat [pool number] [use-vpn 0]

13. If a packet does not match any of the conditions in one of the sequences, a default action is taken. For application-aware routing policy, the default action is to accept nonmatching traffic and forward it with no consideration of SLA. You can configure the default action so that SLA parameters are applied to nonmatching packets:
    vSmart(config-policy-name)# default-action sla-class sla-class-name

14. Apply the policy to one or more sites in the overlay network:
    vSmart(config)# apply-policy site-list list-name app-route-policy policy-name

Structural Components of Policy Configuration for Split DNS

Below are the structural components required to configure split DNS on a vSmart controller. The components related to configuring split DNS are explained in the sections below. For an explanation of the data policy and application-aware routing policy components that are not specifically related to split DNS, see Configure Centralized Data Policy and Configure Application-Aware Routing.

    policy
      lists
        app-list list-name
        (app application-name | app-family application-family)
        site-list list-name
        site-id site-id
        vpn-list list-name
        vpn-id vpn-id
Configure Split DNS

A data policy or an application-aware routing policy for split DNS uses the following types of lists to group related items. You configure these lists under the `policy lists` command hierarchy on Cisco vSmart controllers.
Table 38:

<table>
<thead>
<tr>
<th>List Type</th>
<th>Description</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications and application</td>
<td>List of one or more applications or application families running on the subnets connected to the Cisco vEdge device. Each <code>app-list</code> can contain either applications or application families, but you cannot mix the two. To configure multiple applications or application families in a single list, include multiple <code>app</code> or <code>app-family</code> options, specifying one application or application family in each <code>app</code> or <code>app-family</code>. • <code>application-name</code> is the name of an application. The Cisco SD-WAN software supports about 2300 different applications. To list the supported applications, use the ? in the CLI. • <code>application-family</code> is the name of an application family. It can be one of the following: antivirus, application-service, audio_video, authentication, behavioral, compression, database, encrypted, erp, file-server, file-transfer, forum, game, instant-messaging, mail, microsoft-office, middleware, network-management, network-service, peer-to-peer, printer, routing, security-service, standard, telephony, terminal, thin-client, tunneling, wap, web, and webmail.</td>
<td>`app-list list-name (app application-name</td>
</tr>
<tr>
<td>families</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sites</td>
<td>List of one or more site identifiers in the overlay network. To configure multiple sites in a single list, include multiple <code>site-id</code> options, specifying one site number in each option. You can specify a single site identifier (such as <code>site-id 1</code>) or a range of site identifiers (such as <code>site-id 1-10</code>).</td>
<td><code>site-list list-name site-id</code></td>
</tr>
<tr>
<td>VPNs</td>
<td>List of one or more VPNs in the overlay network. To configure multiple VPNs in a single list, include multiple <code>vpn</code> options, specifying one VPN number in each option. You can specify a single VPN identifier (such as <code>vpn-id 1</code>) or a range of VPN identifiers (such as <code>vpn-id 1-10</code>).</td>
<td><code>vpn-list list-name vpn vpn-id</code></td>
</tr>
</tbody>
</table>

In the Cisco vSmart controller configuration, you can create multiple iterations of each type of list. For example, it is common to create multiple site lists and multiple VPN lists so that you can apply data policy to different sites and different customer VPNs across the network.

When you create multiple iterations of a type of list (for example, when you create multiple VPN lists), you can include the same values or overlapping values in more than one of these list. You can do this either on purpose, to meet the design needs of your network, or you can do this accidentally, which might occur when you use ranges to specify values. (You can use ranges to specify data prefixes, site identifiers, and VPNs.) Here are two examples of lists that are configured with ranges and that contain overlapping values:

- `vpn-list list-1 vpn 1-10`
- `vpn-list list-2 vpn 6-8`
- `site-list list-1 site 1-10`
- `site-list list-2 site 5-15`

When you configure data policies that contain lists with overlapping values, or when you apply data policies, you must ensure that the lists included in the policies, or included when applying the policies, do not contain overlapping values. To do this, you must manually audit your configurations. The Cisco SD-WAN configuration software performs no validation on the contents of lists, on the data policies themselves, or on how the policies are applied to ensure that there are no overlapping values.
If you configure or apply data policies that contain lists with overlapping values to the same site, one policy is applied and the others are ignored. Which policy is applied is a function of the internal behavior of Cisco SD-WAN software when it processes the configuration. This decision is not under user control, so the outcome is not predictable.

**VPN Lists**

Each data or application-aware policy instance is associated with a VPN list. You configure VPN lists with the `policy data-policy vpn-list` or `policy app-route-policy vpn-list` command. The VPN list you specify must be one that you created with a `policy lists vpn-list` command.

**Sequences**

Within each VPN list, a data policy or an application-aware policy contains sequences of match–action pairs. The sequences are numbered to set the order in which data traffic is analyzed by the match–action pairs in the policy. You configure sequences with the `policy data-policy vpn-list sequence` or `policy app-aware-policy vpn-list sequence` command.

Each sequence in a policy can contain one `match` command and one `action` command.

**Match Parameters**

For a data policy or an application-aware routing policy for split DNS, you must the following two match conditions. You configure the match parameters with the `match` command under the `policy data-policy vpn-list sequence` or `policy app-route-policy vpn-list sequence` command hierarchy on Cisco vSmart controllers.

<table>
<thead>
<tr>
<th>Description</th>
<th>Command</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable split DNS, to resolve and process DNS requests and responses on an application-by-application basis</td>
<td><code>dns-app-list list-name</code></td>
<td>Name of an <code>app-list</code> list. This list specifies the applications whose DNS requests are processed.</td>
</tr>
<tr>
<td>Specify the direction in which to process DNS packets</td>
<td>`dns (request</td>
<td>response)`</td>
</tr>
</tbody>
</table>

**Action Parameters**

When data traffic matches the match parameters, the specified action is applied to it. You configure the action parameters with the `action` command under the `policy data-policy vpn-list sequence` or `policy app-route-policy vpn-list sequence` command hierarchy on vSmart controllers.

For application-aware routing policy, the action is to apply an SLA class, which defines the maximum packet latency or maximum packet loss, or both, for DNS traffic related to the application. For information about these action parameters, see Configure Application-Aware Routing.

For a centralized data policy that enables split DNS, configure the following actions. You can configure other actions, as described in Configure Centralized Data Policy.
Table 40:

<table>
<thead>
<tr>
<th>Description</th>
<th>Command</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct data traffic to an Internet exit point on the local router</td>
<td>nat use-vpn 0</td>
<td>—</td>
</tr>
<tr>
<td>Count matching data packets. Counting packets is optional, but recommended.</td>
<td>action count</td>
<td>Name of a counter.</td>
</tr>
<tr>
<td></td>
<td>counter-name</td>
<td></td>
</tr>
<tr>
<td>Redirect DNS requests to a particular DNS server. Redirecting requests is optional, but if you do so, you must specify both actions.</td>
<td>redirect-dns host</td>
<td>For an inbound policy, redirect-dns host allows the DNS response to be correctly forwarded back to the requesting service VPN.</td>
</tr>
<tr>
<td></td>
<td>redirect-dns ip-address</td>
<td>For an outbound policy, specify the IP address of the DNS server.</td>
</tr>
</tbody>
</table>

**Default Action**

If a data packet being evaluated does not match any of the match conditions in a policy, a default action is applied. By default, the data packet is dropped. To modify this behavior, include the `policy data-policy vpn-list default-action accept` command.

**Applying a Policy**

For an application-aware route policy to take effect, you apply it to a list of sites in the overlay network:

vSmart(config)# apply-policy site-list list-name app-route-policy policy-name

When you apply the policy, you do not specify a direction (either inbound or outbound). Application-aware routing policy affects only the outbound traffic on the vEdge routers.

For a centralized data policy to take effect, you apply it to a list of sites in the overlay network:

vSmart(config)# apply-policy site-list list-name data-policy policy-name (all | from-service | from-tunnel)

For split DNS to work, you apply a policy to DNS requests originated from a server VPN. If you are specifying the address of a DNS server for a particular application, the `policy-name` data policy must contain a `redirect-dns ip-address` action that applies to that application.

vSmart(config)# apply-policy policy-name site-list list-name data-policy policy-name from-service

You also apply a policy to DNS responses being returned from the internet. If you included a `redirect-dns` action in the outbound policy, the `policy-name` data policy must contain a `redirect-dns host` action that applies to the proper application.

vSmart(config)# apply-policy policy-name site-list list-name data-policy policy-name from-tunnel

You can apply the same policy to traffic coming from the service VPN and from the tunnel interface between the router and the internet. If the policy specifies use of a specific DNS for a particular application, the policy must contain two sequences for that application, one with a `request-dns ip-address` action and the second with a `request-dns host` action.

vSmart(config)# apply-policy policy-name site-list list-name data-policy policy-name all
**Example Configuration**

The following example shows a data policy that enables split DNS for a number of applications and counts the DNS traffic:

```
vSmart# show running-config policy
policy
data-policy split_dns
   vpn-list vpn_1
   sequence 1
      match
dns-app-list facebook
dns request
   !
   action accept
count facebook_app
   !
sequence 2
match
dns-app-list concur
dns request
   !
   action accept
count concur_app
   !
   nat use-vpn 0
   redirect-dns 75.0.0.1
   !
sequence 3
match
dns-app-list yahoo
   !
   action accept
count yahoo-app
   nat use-vpn 0
   redirect-dns 75.0.0.1
   !
sequence 4
match
dns-app-list salesforce
   !
   action accept
count salesforce
   nat use-vpn 0
   redirect-dns 75.0.0.1
   !
sequence 5
match
dns-app-list twitter
   dns request
   !
   action accept
count twitter
   nat use-vpn 0
   redirect-dns 75.0.0.1
   !
sequence 9
match
dns-app-list dns_list
   dns request
```
! action accept
count dns_app_list_count
nat use-vpn 0
redirect-dns 75.0.0.1
!
!
sequence 10
match
app-list dns_list
!
action accept
count dns_list_count
nat use-vpn 0
redirect-dns 75.0.0.1
!
default-action accept
!
!
lists
vpn-list vpn_1
vpn 1
!
app-list concur
app concur
!
app-list dns_list
app dns
!
app-list facebook
app facebook
!
app-list gmail
app gmail
app gmail_basic
app gmail_chat
app gmail_drive
app gmail_mobile
!
app-list intuit
app intuit
!
app-list salesforce
app salesforce
!
app-list twitter
app twitter
!
app-list yahoo
app yahoo
!
app-list zendesk
app zendesk
!
site-list vedge1
site-id 500
!
!
vSmart# show running-config apply-policy
apply-policy
site-list vedge1 data-policy split_dns all
Configure Transport-Side NAT

NAT allows requests coming from the internal (local) network to go out to the external network, but it does not allow request from the external network to come to the internal network. This behavior means that it is impossible for an external device to send a packet to a device on the internal network. It also means that device in the internal network cannot operate as a server with regards to the external network.

To allow requests from the external network to reach internal network devices, you configure the Cisco vEdge device that sits at the edge of the internal network to be a NAT gateway that performs NAT port forwarding (also called port mapping). You can also create pools of internal network addresses and dynamically or statically map them to other addresses.

Configure NAT Port Forwarding

To allow requests from the external network to reach internal network devices, you configure the Cisco vEdge device that sits at the edge of the internal network to be a NAT gateway that performs NAT port forwarding (also called port mapping). With such a configuration, the Cisco vEdge device sends all packets received on a particular port from an external network to a specific device on the internal (local) network.

To configure NAT port forwarding, define one or more port-forwarding rules to send packets received on a particular port from the external network to an internal server:

```
vEdge(config)# vpn 0
vEdge(config-vpn)# interface ge slot/port
vEdge(config-interface)# nat
vEdge(config-nat)# port-forward port-start port-number1 port-end port-number2 proto (tcp | udp) private-vpn vpn-id private-ip-address ip-address
```

Use the `port-start` and `port-end` options to define the desired TCP or UDP port or range of ports. `port-number1` must be less than or equal to `port-number2`. To apply port forwarding to a single port, specify the same port number for the starting and ending numbers. When applying port forwarding to a range of ports, the range includes the two port numbers that you specify—`port-number1` and `port-number2`. Packets whose destination port matches the configured port or ports are forwarded to the internal server.

Each rule applies either to TCP or UDP traffic. To match the same ports for both TCP and UDP traffic, configure two rules.

For each rule, specify the private VPN in which the internal server resides and the IP address of the internal server. This VPN is one of the VPN identifiers in the overlay network.

You can create up to 128 rules.

**Best Practices for Configuring NAT Port Forwarding**

Configuring NAT port forwarding can, in some circumstances, make the Cisco vEdge device vulnerable to brute-force attacks. The following configuration snippet illustrates a case where the router could fall victim to an SSH brute-force attack:

```
system
  aaa
    auth-order local
interface ge0/0
  description Internet
  ip address 192.168.50.28/28
  nat
    no block-icmp-error
    respond-to-ping
```
This configuration creates a port-forwarding rule for TCP port 22, to accept SSH requests from external devices. By itself, this rule provides no opening for brute-force attacks. (As a side note, enabling SSH on a router interface that is connected to the internet is inherently unsafe.) However, problems can arise because of some of the other commands in this configuration:

- **respond-to-ping**—This command allows the Cisco vEdge device to respond to ping requests that are sent from the external network. These ping requests bypass any NAT port-forwarding rules that you have configured. In this configuration, the external network is the Internet, so ping requests can come from anywhere. It is recommended that you do not configure the NAT interface to respond to ping requests. If you need to test reachability, configure this command temporarily and then remove it once the reachability testing is complete.

- **private-vpn 0**—The SSH requests are sent to the WAN transport VPN, VPN 0. A best practice is to forward external traffic to a service-side VPN, that is, to a VPN other than VPN 0 or VPN 512.

- **private-ip-address 192.168.50.28 and ip address 192.168.50.28/28**—The address of the internal server to which external traffic is being sent is the same as the IP address of the WAN interface. For the private IP address, a best practice is to specify the IP address of a service-side device. If you need to specify a private IP address for one of the interfaces on the Cisco vEdge device, do not use an address in the transport VPN (VPN 0). If you need to use an address in VPN 0, do not use an interface that is connected to the Internet.

- **auth-order local**—This configuration provides only for local authentication, using the credentials configured on the Cisco vEdge device itself. No RADIUS or TACACS server is used to verify the user’s SSH login credentials. While this configuration normally does not expose the router to brute-force attacks, here, in the context of the rest of the configuration, it contributes to the router’s vulnerability to attack.

### Configure NAT Pools

You can configure pools of public IP address and map them to private IP addresses.

First configure a pool of public IP addresses to use for NAT translation:

```
vEdge(config)# vpn 0
vEdge(config-vpn)# interface interface-name
vEdge(config-interface)# nat
vEdge(config-nat)# natpool range-start ip-address1 range-end ip-address2
```

In the address range, `ip-address1` must be less than or equal to `ip-address2`. The pool can contain a maximum of 32 IP addresses. The addresses must be in the same subnet as the interface's IP address.

Then define the address mapping:

```
vEdge(config)# vpn 0
vEdge(config-vpn)# interface interface-name
vEdge(config-interface)# nat
```
In `source-ip`, specify the private source IP address to be NATed. This is the IP address of a device or branch router on the service side of the Cisco vEdge device.

In `translate-ip`, specify the public IP address to map the private source address to. This IP address must be contained in the pool of NAT addresses that you configure with the `natpool` command.

In `source-vpn`, specify the service-side VPN from which the traffic flow is being sent.

In `protocol`, specify the protocol being used to send the traffic flow.

In `source-port` and `translate-port`, specify the number of the source port and the port to which to translate it. The port number can be from 1 through 65535.

You can configure as many static address mappings as there are addresses in the NAT pool.

If you configure a NAT pool but do not configure any static address mappings, NAT translation is done dynamically using the IP addresses in the NAT pool. When a flow terminates, its NATed IP address is released and can be reused.

### Service-Side NAT Configuration Example

In this service-side NAT configuration example, two vEdge routers—vEdge5 and vEdge6—are located at two different sites in the overlay network and connected to each other via the Internet. They are both configured as NATs. Router7 sits in the service side behind vEdge5, and the local network at this site runs OSPF. Router8 sits behind vEdge6 on a network running IBGP.

vEdge5 NATs the source IP address 10.20.24.17, which originates on Router7, translating it to 10.15.1.4. From a NAT perspective on vEdge5, the address 10.20.24.17 is an inside address.

When vEdge6 receives packets with the source IP address 10.15.1.4, it translates the address to 10.16.1.4. From a NAT perspective on vEdge6, the address 10.15.1.4 is an outside address.

In addition, vEdge5 NATs the outside IP source address 10.20.25.18, which originates on Router8 (behind vEdge6), translating it to 10.25.1.1.

The data policies to direct service-side traffic to the NAT are configured on two vSmart controllers, vSmart9 and vSmart10.

By default, OMP advertises all inside NAT pool IP addresses and all static NAT pool IP addresses, so all devices on the overlay network learn these routes automatically. In this example configuration, we configure OSPF and BGP to redistribute outside NAT pool IP addresses. The result is that OSPF on vEdge5 redistributes outside NAT pool IP addresses to its OSPF neighbor, Router7, and BGP redistributes outside NAT pool IP addresses to its BGP neighbor, Router8.
### Configure Service-Side NAT on the vEdge Routers

vEdge5 and vEdge6 are vEdge routers at two different sites. They are both connected to the Internet, and they are both running NAT.

On vEdge5, we configure a NAT pool that can translate four static addresses:

```bash
vEdge5(config)# vpn 1
vEdge5(config-vpn-1)# interface natpool1
vEdge5(config-natpool1)# ip address 10.15.1.4/30
vEdge5(config-natpool1)# no shutdown
```

With this configuration, the following IP addresses are available for static source IP address mapping: 10.15.1.4, 10.15.1.5, 10.15.1.6, and 10.15.1.7.

We then configure NAT on this interface:

```bash
vEdge5(config-natpool1)# nat
```

We want to enforce 1:1 static source IP address mapping:

```bash
vEdge5(config-nat)# no overload
```

If you omit this command, the default behavior is overload, which is effectively dynamic NAT. With the default behavior, all IP addresses are translated to an address in the pool of NAT addresses configured in the ip address command. The addresses are mapped one to one until the address pool is depleted. Then, the last address is used multiple times, and the port number is changed to a random value between 1024 and 65535. Overloading effectively implements dynamic NAT.

For this NAT pool, we want network address translation to be performed only on inside IP source addresses. Inside address translation is the default behavior. You can also explicitly configure it:

```bash
vEdge5(config-nat)# direction inside
```

For this example, we configure two NAT mappings. We want to NAT the source IP address 10.20.24.17, which is the IP address of Router7. This address is an inside address; that is, it is an address at the local site. We also want to NAT the source IP address 10.20.25.18, which comes from Router8, a router behind vEdge6. This is an outside address.

```bash
vEdge5(config-nat)# static source-ip 10.20.24.17 translate-ip 10.15.1.4 inside
vEdge5(config-nat)# static source-ip 10.20.25.18 translate-ip 10.25.1.1 outside
```

We translate the inside source IP address 10.20.24.17 to 10.15.1.4. Because this NAT pool performs NAT only on inside IP source addresses (direction inside), and because 10.20.24.17 is an inside address, the translated address must be one of the addresses in the IP address range 10.15.1.4/30, which is the IP address of the NAT pool interface (configured in the ip address command).

We translate the outside address 10.20.25.18 to 10.25.1.1. Because this NAT pool performs NAT only on inside IP source addresses, we can translate outside addresses to any IP address that is routable on the service-side network behind vEdge6.

At vEdge6, we want to translate the source IP address 10.15.1.4, the translated address received from vEdge5, to an address that is routable on the service network behind vEdge6. The NAT pool that we configure on vEdge6 performs NAT only on outside addresses:

```bash
vEdge6(config)# vpn 1
vEdge6(config-vpn-1)# interface natpool1
vEdge6(config-natpool1)# ip address 10.16.1.4/30
vEdge6(config-natpool1)# no shutdown
vEdge6(config-natpool1)# nat
vEdge6(config-nat)# direction outside
vEdge6(config-nat)# static source-ip 10.15.1.4 translate-ip 10.16.1.4 outside
vEdge6(config-nat)# no overload
```
Here are the complete configurations for the static NAT pools on the vEdge5 and vEdge6 routers:

```plaintext
vEdge5# show running-config vpn 1 interface natpool1

vpn 1
interface natpool1
ip address 10.15.1.4/30
nat
    static source-ip 10.20.24.17 translate-ip 10.15.1.4 inside
    static source-ip 10.20.25.18 translate-ip 10.25.1.1 outside
    no overload
! no shutdown
!
!

vEdge6# show running-config vpn 1 interface natpool2

vpn 1
interface natpool2
ip address 10.16.1.4/30
nat
    static source-ip 10.15.1.4 translate-ip 10.16.1.4 outside
direction outside
    no overload
! no shutdown
!
!
```

**Configure Data Policies on vSmart Controllers**

To direct service-side traffic to the NAT pool interface, you configure centralized data policies on the vSmart controllers. Our example network has two vSmart controllers, vSmart9 and vSmart10. The data policies must be identical on both of them.

The basic structure of the data policy is to define the match criteria for the packets destined to the NAT interface and then, in the action portion of the policy, to assign or direct the packets to a specific NAT pool. The data policy structure looks like this:

```
For a data-policy
For a vpn-list
    For a sequence number
        Match specific criteria
        Action accept
        nat pool number
Apply the data-policy to all data traffic
```

In our example, we want a data policy that directs service-side traffic behind the vEdge5 router to the router's NAT pool interface 1 (interface natpool 1). Here is one portion of the data policy (specifically, one of the sequences within the policy) that does this, defining the service-side traffic by its source and destination IP addresses:

```plaintext
policy
data-policy accept_nat
vpn-list vpn_1
    sequence 108
    match
        source-ip  10.1.17.0/24
destination-ip 10.25.1.0/24
! action accept
    count nat_108
    nat pool 1
!```
This data policy snippet takes data traffic whose source IP address is in the range 10.1.17.0/24 and destination is 10.25.1.0/24, accepts it, counts it to the file nat_108, and directs it to NAT pool 1. The source IP prefix 10.1.17.0/24 corresponds to traffic originating from Router7. The destination IP prefix 10.25.1.0/24 is an IP address that the vEdge5 router has translated from 10.20.25.18. This latter IP address corresponds to data traffic originating on Router8, so data traffic with a destination IP prefix of 10.25.1.0/24 is delivered to vEdge6 and then to Router8.

The second configuration snippet applies the policy to all traffic passing through the router (all).

**Configure Route Redistribution by OSPF and BGP**

By default, OSPF redistributes routes learned from inside NAT pool prefixes into OSPF. In addition, no routes from any other protocols are distributed into OSPF. The same is true for BGP.

In our configuration, we also want OSPF and BGP to redistribute routes learned from outside NAT pool addresses. We also want OSPF to redistribute connected, OMP, and static routes, and we want BGP to redistribute OMP and static routes.

vEdge5# `show running-config vpn 1 router`

```
vpn 1
router
  ospf
    redistribute static
    redistribute connected
    redistribute omp
    redistribute natpool-outside
    area 0
      interface ge0/4
        hello-interval 1
        dead-interval 3
        exit
      exit
    exit

vEdge6# `show running-config vpn 1 router`

```
vpn 1
router
  bgp 1
    timers
      keepalive 1
      holdtime 3
    !
    address-family ipv4-unicast
      redistribute static
      redistribute omp
      redistribute natpool-outside
    !
    neighbor 10.20.25.18
      no shutdown
      remote-as 2
      timers
```
Service-Side NAT Configuration Example

```plaintext
connect-retry 2
advertisement-interval 1
!

Verify the NAT Configuration

You use two commands to verify that the NAT configuration is operational: `show interface` and `show ip nat interface`.

The `show interface` command output indicates which NAT pool interfaces are configured and provides status about them. The command output for the vEdge5 router shows that NAT pool interface 1 is administratively and operationally up. This command output also shows information about the other interfaces configured on vEdge 5.

```
show interface
```

Similarly, on the vEdge6 router, we can check that its NAT pool 2 interface is up:

```
show interface
```

To display information about the NAT pools themselves, use the `show ip nat interface` command. Here is the command output for the vEdge5 router in tabular format and for vEdge6 in nontabular format:

```
vEdge5# show ip nat interface

VPN IFNAME MAP TYPE FILTER TYPE FIB FILTER NUMBER IP POOLS
0 natpool1 endpoint-independent address-port-restricted 0 0 10.15.1.4/30 4
1 natpool1 endpoint-independent address-port-restricted 0 0 10.21.26.15/32 1
2 natpool1 endpoint-independent address-port-restricted 0 0 10.21.27.15/32 1
3 natpool1 endpoint-independent address-port-restricted 0 0 10.21.28.15/32 1
4 natpool1 endpoint-independent address-port-restricted 0 0 10.21.29.15/32 1
5 natpool1 endpoint-independent address-port-restricted 0 0 10.21.30.15/32 1
6 natpool1 endpoint-independent address-port-restricted 0 0 10.21.31.15/32 1
```

```plaintext
1 natpool1 endpoint-independent address-port-restricted 0 0 10.15.1.4/30 4
1 natpool1 endpoint-independent address-port-restricted 0 0 10.21.26.15/32 1
1 natpool1 endpoint-independent address-port-restricted 0 0 10.21.27.15/32 1
1 natpool1 endpoint-independent address-port-restricted 0 0 10.21.28.15/32 1
1 natpool1 endpoint-independent address-port-restricted 0 0 10.21.29.15/32 1
1 natpool1 endpoint-independent address-port-restricted 0 0 10.21.30.15/32 1
1 natpool1 endpoint-independent address-port-restricted 0 0 10.21.31.15/32 1
```

```
vEdge6# show ip nat interface

VPN IFNAME MAP TYPE FILTER TYPE FIB FILTER NUMBER IP POOLS
1 natpool1 endpoint-independent address-port-restricted 0 0 10.15.1.4/30 4
1 natpool1 endpoint-independent address-port-restricted 0 0 10.21.26.15/32 1
1 natpool1 endpoint-independent address-port-restricted 0 0 10.21.27.15/32 1
1 natpool1 endpoint-independent address-port-restricted 0 0 10.21.28.15/32 1
1 natpool1 endpoint-independent address-port-restricted 0 0 10.21.29.15/32 1
1 natpool1 endpoint-independent address-port-restricted 0 0 10.21.30.15/32 1
1 natpool1 endpoint-independent address-port-restricted 0 0 10.21.31.15/32 1
```

```plaintext
1 natpool1 endpoint-independent address-port-restricted 0 0 10.15.1.4/30 4
1 natpool1 endpoint-independent address-port-restricted 0 0 10.21.26.15/32 1
1 natpool1 endpoint-independent address-port-restricted 0 0 10.21.27.15/32 1
1 natpool1 endpoint-independent address-port-restricted 0 0 10.21.28.15/32 1
1 natpool1 endpoint-independent address-port-restricted 0 0 10.21.29.15/32 1
1 natpool1 endpoint-independent address-port-restricted 0 0 10.21.30.15/32 1
1 natpool1 endpoint-independent address-port-restricted 0 0 10.21.31.15/32 1
```
1 natpool13 endpoint-independent address-port-restricted 0 0 10.21.32.15/32 1
1 natpool14 endpoint-independent address-port-restricted 0 0 10.21.33.15/32 1
1 natpool15 endpoint-independent address-port-restricted 0 0 10.21.34.15/32 1
1 natpool16 endpoint-independent address-port-restricted 0 0 10.21.35.15/32 1

vEdge6# show ip nat interface
ip nat interface nat-vpn 1 nat-ifname natpool2
mapping-type endpoint-independent
filter-type address-port-restricted
filter-count 0
fib-filter-count 0
ip 10.16.1.4/30

Verify Routes and Route Redistribution

We configured OSPF and BGP to redistributes routes learned from outside NAT into OSPF and BGP, respectively. (We also configured OSPF and BGP to redistribute static and OMP routes, and we configured OMP to redistribute routes learned from directly connected devices.)

To see where routes have been learned from, look at the Protocol field in the output of the show ip routes command.

Looking on the vEdge5 router, we see that OSPF has redistributed 10.15.1.4/30, a route learned from an inside NAT (these routes are redistributed by default) and 10.25.1.1/32, a route learned from an outside NAT. The vEdge5 router translates the IP address 10.25.1.1 from 10.20.25.18. Both these routes have a next-hop interface of natpool1, which is the NAT pool we configured to run static NAT.

The vEdge6 router translates the outside source IP address 10.15.1.4 to 10.16.1.4. The route table on vEdge6 shows this route and that it has been learned from an outside NAT. The next-hop interface for this prefix is natpool2.
<table>
<thead>
<tr>
<th>VPN</th>
<th>PREFIX</th>
<th>PROTOCOL</th>
<th>NEXTHOP SUB TYPE</th>
<th>IF NAME</th>
<th>ADDR</th>
<th>VPN</th>
<th>TLOC</th>
<th>IP</th>
<th>COLOR</th>
<th>ENCAP</th>
<th>STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0.0.0.0/0</td>
<td>static</td>
<td>-</td>
<td>ge0/0</td>
<td>10.1.16.13</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>F,S</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>10.0.21.0/24</td>
<td>connected</td>
<td>-</td>
<td>ge0/3</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>F,S</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>10.0.100.0/24</td>
<td>connected</td>
<td>-</td>
<td>ge0/7</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>F,S</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>10.1.16.0/24</td>
<td>connected</td>
<td>-</td>
<td>ge0/0</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>F,S</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>10.1.18.0/24</td>
<td>connected</td>
<td>-</td>
<td>ge0/1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>F,S</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>172.16.255.16/32</td>
<td>connected</td>
<td>-</td>
<td>system</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>F,S</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1.1.1.0/24</td>
<td>omp</td>
<td>-</td>
<td>-</td>
<td>172.16.255.14</td>
<td>lte</td>
<td>ipsec</td>
<td>F,S</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>2.2.0.0/16</td>
<td>static</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>B,F,S</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>4.4.4.4/32</td>
<td>omp</td>
<td>-</td>
<td>-</td>
<td>192.16.255.15</td>
<td>lte</td>
<td>ipsec</td>
<td>F,S</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>9.0.0.0/8</td>
<td>static</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>B,F,S</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>10.1.17.0/24</td>
<td>omp</td>
<td>-</td>
<td>-</td>
<td>192.16.255.15</td>
<td>lte</td>
<td>ipsec</td>
<td>F,S</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>10.1.18.0/24</td>
<td>static</td>
<td>-</td>
<td>ge0/4</td>
<td>10.20.25.18</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>F,S</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>10.2.2.0/24</td>
<td>omp</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>F,S</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>10.2.3.0/24</td>
<td>omp</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>F,S</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>10.15.1.4/30</td>
<td>omp</td>
<td>-</td>
<td>-</td>
<td>172.16.255.15</td>
<td>lte</td>
<td>ipsec</td>
<td>F,S</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>10.16.1.4/30</td>
<td>natpool-outside</td>
<td>natpool12</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>F,S</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>10.20.24.0/24</td>
<td>omp</td>
<td>-</td>
<td>-</td>
<td>192.16.255.15</td>
<td>lte</td>
<td>ipsec</td>
<td>F,S</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>10.20.25.0/24</td>
<td>connected</td>
<td>-</td>
<td>ge0/4</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>F,S</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>10.25.1.0/24</td>
<td>omp</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>F,S</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>56.0.1.0/24</td>
<td>omp</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>F,S</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>60.0.1.0/24</td>
<td>connected</td>
<td>-</td>
<td>ge0/5</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>F,S</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>61.0.1.0/24</td>
<td>connected</td>
<td>-</td>
<td>ge0/6</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>F,S</td>
<td></td>
</tr>
<tr>
<td>512</td>
<td>10.0.1.0/24</td>
<td>connected</td>
<td>-</td>
<td>eth0</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>F,S</td>
<td></td>
</tr>
</tbody>
</table>

**View Interface Statistics**

To display packet receipt and transmission statistics for the interfaces, use the `show interface statistics` command. The output shows the following statistics:

```
vEdge5# show interface statistics natpool1 | notab
interface vpn 1 interface natpool1 af-type ipv4
rx-packets 0
rx-octets 0
rx-errors 0
rx-drops 0
tx-packets 0
tx-octets 0
tx-errors 0
tx-drops 0
rx-pps 0
rx-kbps 0
tx-pps 0
tx-kbps 0
```

To display NAT-specific interface statistics, use the `show ip nat interface-statistics` command. The output shows the following statistics for each NAT pool:

```
vEdge5# show ip nat interface-statistics
ip nat interface-statistics nat-vpn 1 nat-ifname natpool1
  nat-outbound-packets 0
  nat-inbound-packets 0
  nat-encode-fail 0
  nat-decode-fail 0
  nat-map-add-fail 0
  nat-filter-add-fail 0
  nat-filter-lookup-fail 0
  nat-state-check-fail 0
  nat-policer-drops 0
  outbound-icmp-error 0
  inbound-icmp-error 0
  inbound-icmp-error-drops 0
  nat-fragments 0
```

---

**Policies Configuration Guide for vEdge Routers, Cisco SD-WAN Releases 19.1, 19.2, and 19.3**

---

**Cisco vEdge Device as a NAT Device**

---

**Service-Side NAT Configuration Example**

EI -> ospf-external, E2 -> ospf-external2, N1 -> ospf-nssa-external1, N2 -> ospf-nssa-external2, e -> bgp-external, i -> bgp-internal

Codes Status flags:
F -> fib, S -> selected, I -> inactive, B -> blackhole, R -> recursive
nat-fragments-fail 0
nat-unsupported-proto 0
nat-map-no-ports 0
nat-map-cannot-xlate 0
nat-filter-map-mismatch 0
nat-map-ip-pool-exhausted 0

View the Data Policy Pushed to the vEdge Routers

To view and verify the data policy pushed from the vSmart controllers to the two vEdge routers, use the `show policy from-vsmart` command. The following is the command output for the vEdge5 router. The output on vEdge6 is identical.

```
vEdge5# show policy from-vsmart
from-vsmart data-policy accept_nat
direction all
vpn-list vpn_1
sequence 100
match
   source-ip 10.20.24.0/24
   destination-ip 10.20.25.0/24
action accept
   count nat
   nat pool 1
sequence 101
match
   source-ip 10.20.24.0/24
   destination-ip 10.1.15.13/32
action accept
   count nat_inet
   nat use-vpn 0
sequence 102
match
dscp 15
action accept
   count nat_dscp
   nat use-vpn 0
sequence 104
match
   source-ip 10.1.18.0/24
   destination-ip 10.20.24.0/24
action accept
   count nat2
   nat pool 1
sequence 105
match
   source-ip 10.1.18.0/24
   destination-ip 10.1.17.0/24
action accept
   count nat3
   nat pool 1
sequence 106
match
   source-ip 10.1.17.0/24
   destination-ip 10.20.25.0/24
action accept
   nat pool 1
sequence 107
match
   source-ip 10.15.1.0/24
   destination-ip 10.20.25.0/24
action accept
   nat pool 2
```
sequence 108
  match
    source-ip 10.1.17.0/24
destination-ip 10.25.1.0/24
  action accept
count nat_108
  nat pool 1
sequence 109
  match
    source-ip 10.20.24.0/24
destination-ip 10.25.1.0/24
  action accept
count nat_109
  nat pool 1
default-action accept
from-vmart lists vpn-list vpn_1
vpn 1

Configurations for Each Network Device
For each of the network devices in this configuration example, this section shows the portions of the
collection relevant to the service-side NAT configuration.

vEdge5 Router
The vEdge5 router is located at site 500, has a system IP address of 172.16.255.15, and has one connection
to the Internet:

system
  host-name vm5
  system-ip 172.16.255.15
  site-id 500
!
vpn 0
  interface ge0/0
    ip address 10.1.15.15/24
tunnel-interface
    encapsulation ipsec
color lte
    hello-interval 60000
    hello-tolerance 120
    no allow-service bgp
    allow-service dhcp
    allow-service dhcpv6
    allow-service dns
    allow-service icmp
    no allow-service sshd
    no allow-service netconf
    no allow-service ntp
    no allow-service ospf
    no allow-service stun
!
    !
    no shutdown
!
!
In VPN 1, NAT pool 1 runs 1:1 static NAT:

vpn 1
  interface natpool1
    ip address 10.15.1.4/30
  nat
    static source-ip 10.20.24.17 translate-ip 10.15.1.4 inside
static source-ip 10.20.25.18 translate-ip 10.25.1.1 outside
no overload
!
no shutdown
!

VPN 1 also has a number of other NAT pool interfaces:

interface natpool10
  ip address 10.21.29.15/32
  no shutdown
!
interface natpool11
  ip address 10.21.30.15/32
  no shutdown
!
interface natpool12
  ip address 10.21.31.15/32
  no shutdown
!
interface natpool13
  ip address 10.21.32.15/32
  no shutdown
!
interface natpool14
  ip address 10.21.33.15/32
  no shutdown
!
interface natpool15
  ip address 10.21.34.15/32
  no shutdown
!
interface natpool16
  ip address 10.21.35.15/32
  no shutdown
!
interface natpool7
  ip address 10.21.26.15/32
  no shutdown
!
interface natpool8
  ip address 10.21.27.15/32
  no shutdown
!
interface natpool9
  ip address 10.21.28.15/32
  no shutdown
!
  ip route 2.2.0.0/16 null0
  ip route 4.4.4.4/32 null0
  ip route 10.1.17.0/24 10.20.24.17
  ip route 10.25.1.0/24 null0
!

OSPF runs in VPN 1 and is configured to redistribute routes learned from outside NAT prefixes into OSPF:

vpn 1
router
  ospf
    timers spf 200 1000 10000
    redistribute static
    redistribute connected
    redistribute osp
    redistribute natpool-outside
    area 0

interface ge0/4
  hello-interval 1
  dead-interval 3
  exit
  exit

vEdge6 Router

The vEdge6 router is located at site 600, has a system IP address of 172.16.255.16, and has one connection to the Internet:

system
  host-name vm6
  system-ip 172.16.255.16
  site-id 600

vpn 0
  interface ge0/0
    ip address 10.1.16.16/24
  tunnel-interface
    encapsulation ipsec
    color lte
    no allow-service bgp
    allow-service dhcp
    allow-service dhcpv6
    allow-service dns
    allow-service icmp
    no allow-service sshd
    no allow-service netconf
    no allow-service ntp
    no allow-service ospf
    no allow-service stun
    !
    no shutdown
    !

VPN 1 has one NAT pool for static address translation:

vpn 1
  interface natpool12
    ip address 10.1.155.4/30
    shutdown
    !
  interface natpool2
    ip address 10.16.1.4/30
  nat
    static source-ip 10.15.1.4 translate-ip 10.16.1.4 outside
dataction outside
    no overload
    !
    no shutdown
    !
  ip route 2.2.0.0/16 null0
  ip route 9.0.0.0/8 null0
  ip route 10.1.18.0/24 10.20.25.18
  !

BGP runs in VPN 1 and is configured to redistribute routes learned from outside NAT prefixes into BGP:

vm6# show running-config vpn 1 router
vpn 1
router
bgp 1
timers
  keepalive 1
  holdtime 3
!
address-family ipv4-unicast
  redistribute static
  redistribute omp
  redistribute natpool-outside
!
neighbor 10.20.25.18
  no shutdown
  remote-as 2
  timers
    connect-retry 2
    advertisement-interval 1
!

Router7 and Router8
Router7 sits in the local site behind the vEdge5 router, and it is an OSPF peer with vEdge5. Router8 sits behind the vEdge6 router and is an IBGP peer with vEdge6.

In our example network, both these routers are configured on vEdge software routers. However, there is nothing in their configuration that specifically relates to static NAT, so we do not show the configurations for these two devices.

vSmart9 and vSmart10 vSmart Controllers
You configure the data policy that runs on the vEdge routers to direct data traffic to the NAT interfaces on the vSmart controllers. The vSmart controllers then push the data policy to the appropriate vEdge routers. The configure data policy must be identical on all vSmart controllers in the overlay network to ensure reproducible data traffic handling in the network.

Here is the complete policy configuration for the two vSmart controllers in our example:

```bash
policy
data-policy accept_nat
  vpn-list vpn_1
  sequence 100
  match
    source-ip 10.20.24.0/24
    destination-ip 10.20.25.0/24
  !
  action accept
  count nat
  nat pool 1
  !
  sequence 101
  match
    source-ip 10.20.24.0/24
    destination-ip 10.1.15.13/32
  !
  action accept
  count nat_inet
  nat use-vpn 0
```
Service-Side NAT Configuration Example

sequence 102
    match
dscp 15
    action accept
count nat_dscp
    nat use-vpn 0

sequence 104
    match
    source-ip 10.1.18.0/24
destination-ip 10.20.24.0/24
    action accept
count nat2
    nat pool 1

sequence 105
    match
    source-ip 10.1.18.0/24
destination-ip 10.1.17.0/24
    action accept
count nat3
    nat pool 1

sequence 106
    match
    source-ip 10.1.17.0/24
destination-ip 10.20.25.0/24
    action accept
    nat pool 1

sequence 107
    match
    source-ip 10.15.1.0/24
destination-ip 10.20.25.0/24
    action accept
    nat pool 2

sequence 108
    match
    source-ip 10.1.17.0/24
destination-ip 10.25.1.0/24
    action accept
count nat_108
    nat pool 1

sequence 109
    match
    source-ip 10.20.24.0/24
destination-ip 10.25.1.0/24
action accept
  count nat_109
  nat pool 1
  !
  !
default-action accept
  !
lists
  vpn-list vpn_1
  vpn 1
  !
site-list east
  site-id 100
  site-id 500
  !
site-list vedge1
  site-id 500
  !
site-list vedge2
  site-id 600
  !
site-list vedges
  site-id 500
  site-id 600
  !
site-list west
  site-id 200
  site-id 400
  site-id 600
  !
  prefix-list prefix_list
  ip-prefix 10.20.24.0/24
  !
  !
vm9# show running-config apply-policy
apply-policy
  site-list vedge1
  data-policy accept_nat all
  !
site-list vedge2
  data-policy accept_nat all
  !
  !
CHAPTER 13

Policy Applications Using CLIs

CLI commands for configuring and monitoring policy applications.

Application-Aware Routing Command Hierarchy

Configure and apply the policy on Cisco vSmart Controllers:

```
policy
 lists
  app-list list-name
    (app application-name | app-family application-family)
    data-prefix-list list-name
    ip-prefix prefix/length
    site-list list-name
    site-id site-id
    vpn-list list-name
    vpn vpn-id
 sla-class sla-class-name
 jitter milliseconds
 latency milliseconds
 loss percentage

policy
 app-route-policy policy-name
  vpn-list list-name
   default-action sla-class sla-class-name
   sequence number
   match
     app-id app-id-name
     app-list list-name
     destination-data-prefix-list list-name
     destination-lp prefix/length
     destination-port number
     dns (request | response)
     dns-app-list list-name
     dscp number
     plp (high | low)
     protocol number
     source-data-prefix-list list-name
     source-lp prefix/length
     source-port number
 action
     backup-sla-preferred-color colors
     count
     log
     sla-class sla-class-name [strict] [preferred-color colors]
```
apply-policy site-list list-name
app-route-policy policy-name

Configure the data plane tunnel performance monitoring parameters on the Cisco vEdge devices:

bfd
  app-route
    multiplier number
    poll-interval milliseconds

Cflowd Traffic Flow Monitoring Command Hierarchy

Configure on Cisco vSmart Controllers only:

policy
  lists
    prefix-list list-name
    ip-prefix prefix/length
    site-list list-name
    site-id site-id
    vpn-list list-name
    vpn vpn-id
  cflowd-template template-name
    collector vpn vpn-id address ip-address port port-number transport transport-type
    flow-active-timeout seconds
    flow-inactive-timeout seconds
    flow-sampling-interval number
    template-refresh seconds

policy
data-policy policy-name vpn-list list-name
  default-action action
  sequence number
  match
    destination-data-prefix-list list-name
    destination-ip prefix/length
    destination-port number
    dscp number
    protocol number
    source-data-prefix-list list-name
    source-ip prefix/length
    source-port number
  action
    count counter-name
    drop
    accept
    cflowd

apply-policy
  site-list list-name
  data-policy policy-name direction
  cflowd-template template-name

Local Internet Exit Command Hierarchy

Configure and apply a centralized data policy on the Cisco vSmart Controller:

policy
  lists
    prefix-list list-name
    ip-prefix prefix/length
    site-list list-name
    site-id site-id
    vpn-list list-name
    vpn vpn-id
cflowd-template template-name
  collector vpn vpn-id address ip-address port port-number
  flow-active-timeout seconds
  flow-inactive-timeout seconds
  template-refresh seconds

policy
data-policy policy-name vpn-list list-name
  default-action action
  sequence number
    match
      destination-data-prefix-list list-name
      destination-ip prefix/length
      destination-port number
      dscp number
      protocol number
      source-data-prefix-list list-name
      source-ip prefix/length
      source-port number
    action
      count counter-name
      drop
      accept
      nat use-vpn 0

apply-policy
  site-list list-name
  data-policy policy-name direction

On a Cisco vEdge device, enable NAT functionality in the WAN VPN:

vpn vpn-id
  interface interface-name
    nat
      refresh (bi-directional | outbound)
      tcp-timeout minutes
      udp-timeout minutes

Zone-Based Firewalls

policy
  lists
    prefix-list list-name
    ip-prefix prefix/length
  tcp-syn-flood-limit number
  zone (destination-zone-name | source-zone-name)
    vpn vpn-id
    zone-to-no-zone-internet (allow | deny)
    zone-pair pair-name
    source-zone source-zone-name
    destination-zone destination-zone-name
    zone-policy policy-name
    zone-based-policy policy-name
  default-action action
  sequence number
    match
      destination-data-prefix-list list-name
      destination-ip prefix/length
      destination-port number
      protocol number
      source-data-prefix-list list-name
      source-ip prefix/length
      source-port number
    action
      drop
Operational Commands

clear app cflowd flow-all (on Cisco vEdge devices only)
clear app cflowd flows (on Cisco vEdge devices only)
clear app cflowd statistics (on Cisco vEdge devices only)
clear policy zbfw filter-statistics (on Cisco vEdge devices only)
clear policy zbfw global-statistics (on Cisco vEdge devices only)
clear policy zbfw sessions (on Cisco vEdge devices only)
show app-route stats (on Cisco vEdge devices only)
show app cflowd collector (on Cisco vEdge devices only)
show app cflowd flow-count (on Cisco vEdge devices only)
show app cflowd flows (on Cisco vEdge devices only)
show app cflowd template (on Cisco vEdge devices only)
show ip routes (on Cisco vEdge devices)
show policy from-vsmart (on Cisco vEdge devices only)
show policy zbfw filter-statistics (on Cisco vEdge devices only)
show policy zbfw global-statistics (on Cisco vEdge devices only)
show policy zbfw sessions (on Cisco vEdge devices only)
show running-config (on Cisco vSmart Controllers only)